H2020 - INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

ICT-11-2017 Collective Awareness Platforms for Sustainability and Social Innovation – Innovation Action (IA)

Child Rescue

"Collective Awareness Platform for Missing Children Investigation and Rescue

D1.2 – Regulatory framework for data protection, privacy, and ethical issues

Workpackage:	WP1 – ChildRescue Operational Requirements and Methodology Definition
Authors:	TSoC, CF, HRC, NTUA, UBITECH
Status:	FIMAL
Date:	30/04/2018
Version:	1.00
Classification:	Public

ChildRescue Project Profile

Grant Agreement No.:	780938
Acronym:	ChildRescue
Title:	Collective Awareness Platform for Missing Children Investigation and Rescue
URL:	http://www.childrescue.eu
Start Date:	01/01/2018
Duration:	36 months

Partners

	National Technical University of Athens (NTUA), Decision Support Systems Laboratory, DSSLab Co-ordinator	Greece
Missing Children Europe	European Federation for Missing and Sexually Exploited Children AISBL - Missing Children Europe (MCE)	Belgium
The smile of the child. CARE. DIGNITY. EQUALITY.	The Smile of the Child (SoC)	Greece
Child Focus 116000	Foundation for Missing and Sexually Exploited Children – (Child Focus)	Belgium
Ελληνικός Ερυθρός Σταυρός	Hellenic Red Cross (REDCROSS)	Greece
FRANKFURT UNIVERSITY OF APPLIED SCIENCES	Frankfurt University of Applied Sciences (FRA-UAS)	Germany
SingularLogic Innovation at your doorstep	SingularLogic ANONYMI ETAIREIA PLIROFORIAKON SYSTIMATON KAI EFARMOGON PLIROFORIKIS (SILO)	Greece
UBITECH ubiquitous solutions	Ubitech Limited (UBITECH)	Cyprus
MADE by MADEGROUP.CO	MADE Group (MADE)	Greece
Suite5 We Deliver Intelligence	SUITE5 DATA INTELLIGENCE SOLUTIONS LTD (SUITE5)	Cyprus

Document History

Version	Date	Author (Partner)	Remarks
0.1	12/3/2018	A. Ntinapogias & A. Gyftopoulou (TSoC)	ToC
0.11	21/03/2018	Christos Ntanos (NTUA)	Reviewed ToC and updated template
0.2	6/4/2018	A. Gyftopoulou & Antonia Tsirigoti (TSoC)	Added legal framework
0.3	13/4/2018	A. Ntinapogias & Antonia Tsirigoti (TSoC)	Added ethical part
0.4	13/04/2018	Christos Ntanos (NTUA)	Added details of platform
0.5	13/04/2018	Dimitris Ntalaperas (Ubitech)	Added details of platform
0.6	18/4/2018	Nel Broothaerts - Child Focus	Added Belgian legal framework
0.7	18/4/2018	Zefi Thanasoula - Hellenic Red Cross	Added information concerning UAMs and performed review
0.75	19/4/2018	Gail Rego (MCE)	Review
0.8	20/04/2018	Christos Ntanos (NTUA)	Draft Ready for review by the EAB
0.9	30/04/2018	Christos Ntanos (NTUA)	Added EAB Report in Annex and performed review
1.0	30/04/2018	Evmorfia Biliri (NTUA)	Quality Control

Executive Summary

This deliverable is part of ChildRescue WP1 – ChildRescue Operational Requirements and Methodology Definition and specifically, it represents the work conducted for T1.2 – Regulatory Framework for Data Protection, Privacy and Ethical Issues.

The aim of this deliverable, according to the DoA, is to ensure that ChildRescue R&D activities comply with established practices as well as the legal framework for ethical, privacy and data protection issues. In this way, it identifies restrictions in relation to privacy and data protection as well as to access to personal information. The goal is to ensure that the methods, tools, technologies and processes proposed by ChildRescue partners will be able to be adopted without any legal barrier to the piloting countries, at least. This includes the terms for obtaining access to data at various confidentiality levels (e.g. anonymized clues, testimonials and social networks data, etc.) and the consent for end-users' participation in ChildRescue tests and pilots, providing the opportunity to withdraw from such activities at any time without any risk for their dignity and privacy.

The deliverable includes the state-of-play of data protection, privacy and ethical issues related to the missing children investigation cycle. The deliverable clarifies how consent/assent will be ensured in case children and/or adults unable to give informed consent are involved and provide details about the measures taken to prevent the risk of enhancing vulnerability/stigmatisation of individuals/groups.

An update of the present deliverable is organised for the second year of the project and specifically M21.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Introduction

ChildRescue is guided by the vision to reduce the primary time between the moment a child is reported missing and the one when it is found, by developing an integrated methodology that will transform the way missing children investigations are currently held. At the same time, it aims to enhance the coordination between hosting facilities and NGOs running hosting facilities for unaccompanied migrant minors to track the relocation of those minors between hosting facilities and countries, even if they present themselves without identification, or new identification papers when reaching another destination, aiming to predict, prevent, and act effectively to protect their best interests in case of a disappearance. In this respect, it places particular emphasis on the study of current AS-IS procedures and the exploration of TO-BE future improved scenarios, and the extraction thereby of the requirements that will make this transformation possible. The present deliverable is released within the context of Work Package 1 "ChildRescue Operational Requirements and Methodology Definition" and is particularly associated with Task 1.2 "Regulatory Framework for Data Protection, Privacy and Ethical Issues".

Aiming to ensure that ChildRescue R&D activities comply with established practices as well as the legal framework for ethical, privacy and data protection issues, this deliverable identifies restrictions in relation to privacy and data protection as well as to access to personal information. The goal is to ensure that the methods, tools, technologies and processes will be able to be adopted without any legal barrier to the piloting countries, at least, which are Greece and Belgium.

Thus the deliverable includes the state-of-play of data protection, privacy and ethical issues related to the missing children investigation cycle.

Recognising the high importance of data privacy in such a research activity, the consortium has put together an Ethics Advisory Board (EAB) comprising of known domain experts and practitioners who will work closely with the overall consortium during the course of the project on tackling ethical and data privacy issues that will have to do with the retrieval, the processing, and the retaining of these data. The EAB will provide independent opinions and thoughts and will advise both the technical and the research partners on issues regarding the ChildRescue methodology, the development of the platform and its components and the piloting operation. In this context, the consortium is complemented with a group of experts who will enhance the expertise in these domains. This deliverable will be independently assessed by EAB.

1.2 Definition of main terms

Below are provided definitions on main terms.

Child: any individual below the age of majority (also minor, juvenile, infant); the age of majority, which transforms a child legally into an adult, has traditionally been the age of 18 years.

Missing child: any child, under 18 years of age, whose whereabouts are unknown by his/her custodial parent(s) or legal guardian(s);[1] in the context of ChildRescue any underage person reported as missing the personal data of which are to be uploaded in the relevant application.

Missing child categories[2]

Endangered Runaway: a child who is away from home without the permission of his or her parent(s) or legal guardian(s). The child may have voluntarily left home for a variety of reasons.

Family Abduction: the taking, retention, or concealment of a child or children by a parent, other family member, custodian, or his or her agent, in derogation of the custody rights, including visitation rights, of another parent or family member.

Non-Family Abduction: the coerced and unauthorized taking of a child by someone other than a family member

Lost, Injured, or Otherwise Missing: a child who has disappeared under unknown circumstances. Facts are insufficient to determine the cause of a child's disappearance.

Abandoned or Unaccompanied Minor: a child who is not accompanied by an adult legally responsible for him or her, including those traveling alone without custodial permission, those separated by an emergency, those in a refugee situation, and those who have been abandoned or otherwise left without any adult care.

Family: In Greece, Law 3500/2006 on combating domestic violence, Article 1, Para 2: Family a. consists of spouses or parents and relatives first and second degree by blood or by marriage and by adoptive children; b. includes, where there is cohabitation, relatives by blood or marriage up to the fourth degree and persons whose guardian, court attendant or foster parent are designated as a family member, and any minor person who lives in the family; c. the provisions of this Law apply to a permanent companion of the man or the woman and the children, common or one of them, provided they cohabit. Also applies to the former husbands and wives][3]

The Belgian law defines a family as 'every group of persons which are partners or relatives and who are economically dependent from each other'. A group of family members can consist of the partners and blood relatives of (one of the) partners. The law of August 12th 2000 concerning social,

[1] Source: https://www.icmec.org/global-missing-childrens-center/definition-of-missing/#Greece

[2] Source: https://www.icmec.org/global-missing-childrens-center/the-definition-of-missing/

[3] Source: http://www.can-via-mds.eu/sites/default/files/WS%202_D4.c_CAN-MDS%20Toolkit_Operator%27s%20Manual_Master%20Toolkit.pdf

budgetary and other provisions defines that two (or more) persons form an actual family if they live together at the same address and organise a household together while both financially contributing to it. They are not necessarily married and it doesn't matter whether they have the same sex or not. Special provisions are foreseen for single parent families where a child is raised by just one of parents by blood. Also foster children are considered member of the family when they live during a specific period of time at the same address.

> **Foster family**: a family where the child lives for a specific period of time along with adults that are not related within the first degree of consanguinity or affinity to him/her and who officially takes one or more children into their family, cared for and maintained, for compensation or otherwise, including the provision of permanent free care without becoming the child's legal parents. The child is referred to as their foster child[4]

Parent: custodial or noncustodial biological or adoptive parent of the child (reported as missing); a person who has a legal parent and child relationship with a child which confers or imposes on the person legal rights, privileges, duties, and obligations[5]

> **Custodial parent**: having the responsibility for the care and control of the child and for the child's overall health and welfare
>
> **Noncustodial parent**: not having the responsibility for care and control of the child or for the child's overall health and welfare
>
> **Adoptive parent**: a person who adopts a child born by other parents as his or her own child via the "adoption" process
>
> **Foster parent**: a person who acts as a custodial parent for a child in place of the child's natural parents but without legally adopting the child; this is fostering care

Agency: in the context of the ChildRescue, it is considered any public, semi-public or private organisation or service activated in a related sector in regards to administrative procedure of missing children cases[6]

Agencies related to ChildRescue: any agency involved in the investigation process for identify a missing child; it could be Law Enforcement related Service, as the police; Child Protection/ Social Welfare Services including Accredited NGOs (such as the 116000 line); Judicial Services (such as the juvenile attorney); Mental Health & Health Care Services (primary, secondary & tertiary); Educational Services (preschool, primary & secondary, public & private); already existing Registries including missing children cases (such as Red Cross); Independent Authorities (such as a Child Ombudsman);

[4] Ibid

[5] Ibid

[6] Ibid

and Community Organisations providing one or more relevant services (such as Samaritians, rescue teams etc).

Helpline personnel: this could be a psychologist, counsellor, social worker, community nurse (to be adapted per country)[7]

Helpline: a telephone line operated by a public or charitable organisation providing information, counselling, advice and comfort to worried or unhappy people and help with a variety of problems on the phone[8]

Location: the place or area where the reported missing child seemed last time; it could be: home, day care institution; residential care institution; school; educational institution; health care organisation; detention or correctional institution; recreational or leisure area or a playground; sports-athletics; public transportation means; public place

Ethics: commonly agreed and accepted principles and provisions for ensuring non-conflict between individual and collective interests and rights[9]

Ethics in the ChildRescue: operation oriented to the missing child interests, respecting of human rights and in accordance to relevant legal provisions including the administration of sensitive personal data

Code of ethics: a guide of principles designed to help professionals conduct their tasks honestly, with integrity, transparency, accountability, confidentiality, objectivity, respectfulness, obedience to the law and loyalty[10]

Code of practice: a code adopted by a profession or by a governmental or non-governmental organisation to regulate that profession and may be styled as a code of professional responsibility, which deals with difficult issues, difficult decisions that will often need to be made, and provide a clear account of what behavior is considered "ethical" or "correct" or "right" under the circumstances[11]

Mobile application: A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited function. A mobile application also may be known as an app, Web app, online app, iPhone app or smartphone app.[12]

---

[7] Ibid

[8] Ibid

[9] Ibid

[10] Ibid

[11] Ibid

[12] Source: https://www.techopedia.com/definition/2953/mobile-application-mobile-app

Platform: A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In personal computing, a platform is the basic hardware (computer) and software (operating system) on which software applications can be run. Computers use specific central processing units (CPUs) that are designed to run specific machine language code. In order for the computer to run software applications, the applications must be in that CPU's binary-coded machine language. Thus, historically, application programs written for one platform would not work on a different platform.[13]

Anonymisation: the processing of personal data with the aim of irreversibly preventing the identification of the individual to whom it relates. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.[14]

The definition of the terms, '**user**', '**traffic data**', '**location data**', '**communication**', '**personal data'**, '**pseudonymisation**', '**data subject**', '**processing (of data)**', '**profiling**', '**filling system (for personal data)**', '**controller (of personal data)**', '**processor (of personal data)**', '**recipient (of personal data)**', '**third party**', '**consent of the data subject**', '**personal data breach**', '**genetic data**', '**biometric data**', '**data concerning health**' is included in chapter 3.

[13] Source: https://www.techopedia.com/definition/3411/platform

[14] Source: https://www.dataprotection.ie/docs/Anonymisation-and-pseudonymisation/1594.htm

2 Overview of main properties of ChildRescue Platform

2.1 Description of ChildRescue Platform: concept

The ChildRescue platform follows a tiered approach. Though the complete specification of the ChildRescue architecture will be carried through in WP3, the broad functionalities for each layer of the architecture and the way in which data protection will be ensured by the relevant layers can be given at this stage.

2.1.1 Layers

The main layers of the ChildRescue are depicted in **Error! Reference source not found.**. The Data layer is responsible for storing data while the Logic and Presentation layer are responsible for performing business logic and graphical output respectively. The layers are connected via a set of interfaces. The most important interface concerning data protection is the Data Interface. This interface, apart from exposing data to the business layer, will also perform encryption and anonymizing operations where applicable. Anonymization will be performed exclusively on the Data Interface, so that no plain data will reach the business logic layer. Data fragmentation will also be performed on the Data Interface so that if data that are fragmented will be requested, the data will be securely and transparently be reassembled before reaching the Business Logic Layer.

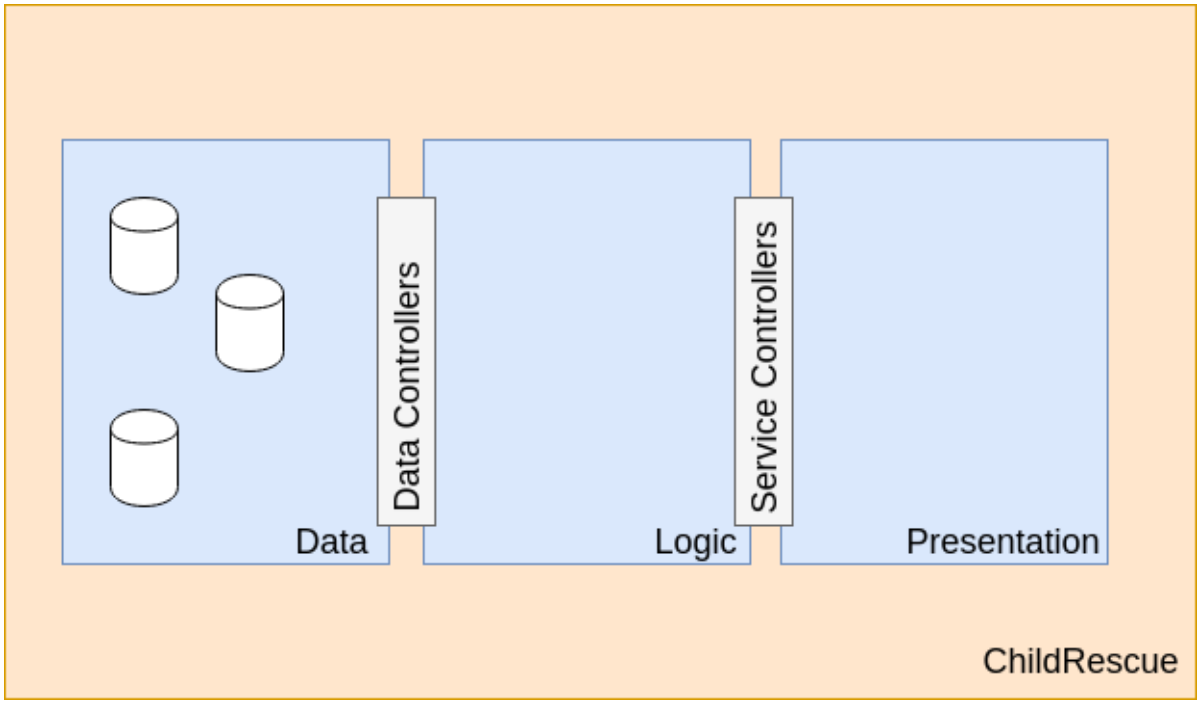

Figure 2-1: Main Layers of the ChildRescue Architecture

2.1.2 Usages (**primary**-investigation for missing children **and secondary** usages of data-profiling; identifying patterns; extraction of lessons learned; retrieval of similar cases; statistics)

For the organisations, the main usage of the ChildRescue platform will be to provide support for the investigation of missing children or unaccompanied minors cases by centralizing the organisation's data and enhancing the communication between organisation departments as well between the organisation and volunteers and teams operating in the field. Supporting this main usage, ChildRescue will furthermore deploy a set of algorithms to identify rules and patterns combining data from profiles, past cases and social media. The extracted results will be used to generate suggestions based on present and past knowledge and constructing useful non-trivial statistics that will come from combining similar cases and significant events.

2.1.3 Functions (profiling methods; semantic extraction of tags; sentiment analysis; social network analysis; applying activity theory principles and predictive analytic methods)

Though the description of functions that will be implemented by the ChildRescue platform will be fully specified during WP 3, the broad categories of the functions to be implemented can be summarized as:

- Central functions: These functions achieve the efficient communication both between the organisation and external entities, such as cooperating agencies and volunteers, as well as interorganisational communication between departments. Data storage, organisation, harmonization and centralization are also part of the core functions.

- Profiling functions: These functions achieve the efficient storage and semantic enrichment of cases' profiles.

- Social media functions: These functions are responsible for retrieving public posts from monitored social media accounts and performing unit analysis. Unit analysis in this context, means analysis of the post that is not dependent to other entities such as other posts or profile information. Examples of this kind of analysis are sentiment analysis, named entity recognition etc.

- Predictive analysis: These functions combine profile and historical data as well as data being originated from social media and provide suggestions and predictions based on them. Based on the configuration that the user chooses, when new correlations are generated (for example when a new post in facebook drives the analysis engine to produce a significant result) the output can also be pushed to operators by the generation of appropriate alerts.

2.2 Description of subjects of data

This chapter describes the data of each stakeholder that is inserted and stored on the ChildRescue platform. Different data will be stored on the platform depending on the stakeholder. At this stage, the following data is indicative. Following the further development of the project and the analysis to

be performed in "WP2 - Grassroot Collective Intelligence in the Missing Children Investigation" this chapter is going to be expanded with the update of this deliverable in M21.

In the investigation cycle, the main subjects of data collection and processing are the missing children and the unaccompanied migrant minors, where informed consent can be challenge. As this is out of the scope of the project and would make data collection significantly more difficult to achieve, the platform will collect or store no biometric data for any of its users or data subjects. Any validation of user accounts for organisational roles (e.g. members of volunteer organisations, organisation managers etc.) will happen offline using processes already in place. A central premise about the availability of data concerning specific cases, is that it will not extend beyond its direct and measurable usefulness. When a platform user is no longer needed to have access to profiling data, availability and traces of that availability on devices where it was accessed is removed.

2.2.1 Missing children (end beneficiaries of ChildRescue Platform)

Missing children are the end beneficiaries of the platform. They are the target of the investigation mission. In most cases they will not be direct users of the platform, but all actions revolve around them. A child is considered legally missing when a report of its disappearance has been filed to the appropriate authorities.

When there is a missing child's case, the case file will be created and added on the platform. The case file will include personal and psychosocial information of the child. The missing child's indicative data that will be stored include: name, surname, sex, date of birth, physical description, eye colour, hair colour, height, weight, last clothes worn, the last place the child had been seen, information mined from public social media profiles and activities of the child for identifying activity and mobility patterns, a recent photograph, any health issues, places recently visited, interests, etc. Additional information about the missing child could possibly include social background, habits, mental health, etc. This data will be stored to assist in the organisation's experts to build a psychosocial profile of the missing child.

Access to the complete data set for each case will only be given to the responsible organisation's management actors and organisation owner. Distribution of part of that information will be towards validated users holding organisational roles on a case-by-case basis when authorisation is allowed and given, and towards the general public, following the current legal procedure for the issuing of Amber Alters and public missing children alerts.

2.2.2 Unaccompanied migrant minors (end beneficiaries of ChildRescue Platform)

Accommodation of Unaccompanied Minors (Profiling Stage)

All foreign national or stateless persons below the age of 18, who either arrive in the EU unaccompanied by a responsible adult or are left unaccompanied after their arrival, are considered unaccompanied minors. Most of them come from countries at war and/or poor living conditions.

In ChildRescue, unaccompanied migrant minors profiles will be an extension to that of missing children. Basic information about the minor such as name, surname, father's name, mother's name, date of birth, photograph, citizenship, sex, if the minor has passport or not, history of hosting facilities the minor was placed, social media profiles, mobile phone and other contact information etc. will be kept, some of which may be subject to approval or given consent by the subject.

ChildRescue will include profiling information, either entered or derived from automatic calculations or psychological, behavioural or other evaluations, such as if they are under 15 years old, contacts in their home country, current country or destination country, current participation in education activities, additional vulnerability flags (unaccompanied child, separated child, disabilities, risk of trafficking or exploitation, psychological issues, medical health issues, early marriage, mental health issues, risk of actual abuse, etc.), if they have lack of interest in activities, difficulties adapting to their new environment, distant or aggressive behaviour, declaration that another country or city is their final destination, probable geographic routes that he may follow, history or reports of receiving violence and sexual and/or psychological abuse, being marginalised in the reception classes they attend, psychological issues, being pushed into delinquent behaviour etc.

Access to the complete data set for each case will only be given to the responsible organisation's management actors and organisation owner, including the Hosting Facilities Manager, further to the data stored for missing children.

Tracing and Search & Rescue

One special case regarding unaccompanied migrant minors and ChildRescue is if a minor hosted in one of the facilities managed by the operating organisation has left voluntarily from the facility and a tracing request has been placed with the organisation by a close relative or a legal guardian that has been proven to be operating for the sought person's best interest. Technically this is differentiated from a missing person's report in the sense that the minor being traced is not considered legally missing, the authorities aren't notified, there is no broadcasting of alerts and information flow is heavily restricted to only specific caseworkers. The aim of the process is not to retrieve/apprehend any person, but to restore or create some communication channel between the two parties.

When such a tracing request has been validated by the operating organisation as legitimate and to the best interest of the minor, additional information may be used to search for and/or expand the profile of the minor in ChildRescue. These data include the identity of the person(s) who requested the tracing, more information about the timeline of separation. When and if there is reason anticipate a probable loss of life, additional descriptive non-biometric data may be collected by interviewing the person placing the request, including physical description, distinguishing features, e.g. visible skin marks (scars, tattoos, birthmarks, etc.), visible medical characteristics (injuries, malformation, etc.), dental distinguishing features: (missing front teeth, gold teeth, etc.), what the sought person was wearing (jewellery, watch, etc.), the existence but not the content of identity documents (identity card, driving license, credit card) the person might have been carrying on them, details of type of clothes, etc.

A second special case regarding unaccompanied migrant minors concerns catastrophic events in or near hosting facilities where they reside. In this case, depending on local legislation, public, but

localised alerts could be decided to be raised and dissemination of profiling information further to the alerts could be performed towards Search & Rescue teams and other supporting volunteer teams that are to be directly involved.

2.2.3 Sources of referrals and of further information and at the same time subjects of data including

2.2.3.1 Parents/guardians/tracing applicants

The providers of information on missing children cases and tracing requests are usually close relatives or legal guardians of the children and minors. Any data collected about them is done directly by them through interviews, either in person or by phone, and is stored as a supplement to the profile of the child/minor. That may include name, sex, contact information, relation to the person in the profile and profiling information about them that might be of interest, derived from psychological, behavioural or other evaluations by the caseworkers.

2.2.3.2 Professionals working on specific cases, but are not platform users, either within the operating organisation or outside it (psychologists, social workers, the police, pubic prosecutors etc.)

When professionals are involved in the collection of data about the profiling for specific cases, typically without themselves being platform users, their contribution will be referenced by name. If other information, like contact details, is deemed necessary to be included, it will in a case-by-case basis.

2.2.3.3 'Community sensors'

Registered identifiable users, registered users (without personal identifiers) and anonymous users are considered the community sensors. They will assist in identifying the location of a missing person. Their interactions with the platform with specific intent to communicate information towards it will be logged.

2.2.3.3.1 Registered identifiable users

This category includes the members of the organisations' volunteer teams and other trusted collaborators who are registered and validated. The data that will be stored on ChildRescue is their name, surname, contact details, organisation, role in the organisation, qualifications etc.

2.2.3.3.2 Registered users (without personal identifiers)

This category includes the users who are registered in the platform, either anonymously or eponymously but their identities hasn't been validated. The data stored contain the same fields as the registered identifiable users, but less of them will be required for operating the platform.

2.2.3.3.3 Anonymous users

This category includes the users that land on the ChildRescue platform page or install the mobile application without creating an account. Data stored about these users will be limited to the specific interactions they have with the platform with the specific intent to transmit information (i.e. filling in a contact form or supplying an eye-witness report). A two way communication channel may be required to be formed, but nothing more than the information contained in the message and its headers necessary for supplying it will be used or stored.

2.2.4 Professionals operating the system (voluntary organisations, rescue teams)

The roles of ChildRescue users with administrative or operational roles within the organisations, tasked to perform actions regarding cases stored in the system and for only the organisation they are registered to, are the Hosting Facility Managers, the Organisation Case Managers, the Organisation Network Managers, the Organisation Coordinator, and the Organisation Owner. These are registered identifiable users of the platform whose identities have been validated. Special roles and access to data is provided for them, so their profile information may be required to be more extensive. Thematic, geographic or other organisational responsibilities, further to the organisational role may be stored.

2.2.5 IT Professionals

There are two categories of subjects that are documented in the platform as IT professionals: Platform Developers/Testers and Platform Administrators, that may refer to the same person, under a general user role of Platform Administrator.

Platform Developers aren't required to have user accounts on the platform but are expected to act as testers of various roles, including that of the Platform Administrators.

Platform Administrators will be operationally activated after the launch of he platform and will have control over organisations and the platform, but not their case data.

All information stored for these subjects (roles) falls within the wide range of other kinds subjects, but when on an operational non-testing environment acting as Platform Administrators will be required to be within the scope of what is stored for registered identifiable users.

2.3 Description of data to be collected, shared and processed

Data used in the context of ChildRescue come from a variety of sources and can be of a very diverse nature and can thus be subject to different regulations. Depending on the situation, it may be further required that personal information of the user generating the data is also protected.

The detailed specification concerning technical aspects of the collection, sharing and processing will be the outcome of Task 2.3. For the purposes of the current deliverable, the various techniques that will be used to ensure data privacy can be described in general terms. These are:

- Anonymization, where the source data will be transformed in such a way so that the informational content of the original data set will not be exploitable by a malicious user.

- Blockchains in which newly and previously authorised users will have access to the shared information of the blockchain, until the blockchain owner (typically an organisation) invalidates it.

- Pseudonyms that will guarantee that the personal information of a registered user are not exposed publicly.

- Restriction, where apart from any other applied techniques, the data become by physical or digital means unavailable to the user.

- Controlled Access, typically enforced in the users of an organisation limits the amount of data accessible according to the role of the user.

Apart from the above, there are also freely accessible data that can be accessed without restrictions by a user group.

As previously noted the techniques depend on the source and nature of the data. Table 2-1 summarizes the various levels of protection for each category of users and each type of data. More specifically:

- Social Media Data originate for monitored accounts. While the posts and information are in any case public, to avoid any association between the content and the details of the missing person and since this information is of no use to users outside the organisation, these data are restricted to registered and unregistered users and are being accessed by the organisation in a controlled way.

- Analytics that arise from Social Media analysis and from Profile and previous case analysis are also restricted to the public and allow controlled access from members of the organisation.

- Organisation Public Data consisting of information that the organisation releases to the public are, of course, freely accessible by all.

- Organisation Private Data refers to any data that the organisation has and are not linked directly to any active case. Data like staff details, personal data of the informants belong to this category. These data have controlled access by the members of the organisation and will furthermore be able to be anonymized to ensure maximum security.

- Protected Case data refers to any data being relevant to an active case but are not freely available to the ChildRescue users. The organisation has controlled access to this kind of data, which are further anonymized for extra security. Registered users can also have access to this data via a blockchain, if the organisation authorizes it, so that the integrity of the evidence relevant to the case can be verified. The Blockchain will be operated by the organisation and it will provide the history of the generated evidence to all the users that are

subscribed to it. It will be invalidated by the organisation as soon as the emergency expires. Unregistered users have no access to this kind of data.

- Shared case data refers to any data being relevant to an active case and are also available to the users of the ChildRescue platform. Blockchain, in a similar fashion with the Protected Case data, and anonymization techniques will be performed on this data to ensure that only users of the platform have the required level of access.

- User personal data refers to personal information of the user. Organisation users use internal credentials while unregistered users use no credentials at all; consequently this case in not relevant to them. Registered users on the other hand may use pseudonyms so that the system recognizes them, without any of their personal details becoming exposed.

Table 2-1: Levels of data access

	Social Media Data	Analytics	Organisation Public Data	Organisation Private Data	Protected Case data	Shared case data	User personal data
Organisation	Controlled	Controlled	Free	Controlled, Anonymization	Controlled, Anonymization, Blockchain	Controlled, Blockchain	N/A
Registered user	Restricted	Restricted	Free	Restricted	Blockchain, Anonymization	Blockchain, Anonymization	Pseudonyms
Unregister user	Restricted	Restricted	Free	Restricted	Restricted	Blockchain, Anonymization	N/A

2.3.1 Define roles, rights and accountabilities

The users of the organisation will have controlled access to a variety of information that will be stored internally to databases within the organisation. The level of access, as well as the associated responsibilities will depend both on the user role and on the nature of data. The roles of the users within the organisation can be briefly summarized as:

- Data owner which is the role of the users that can create new data.

- Data processer which is the role of the users that can perform analysis on stored data

- Data management which is the role of the users that perform maintenance and management operations on the data

In the following subsections the rights and responsibilities for each type of user is further analysed.

2.3.1.1 Data owner

A Data owner is a user that can create new data. New form data to a new case of missing child or transfer data of an unaccompanied minor to a new facility are examples of this kind of data. A Data owner is responsible for the validity of the stored data at any point in time by updating them

accordingly. The Data owner has thus full rights to the data she/he created and can perform any update operation needed. The actions performed will be audited by the database so a full history of the data may also be retrieved the data owner or any administrator of the platform. The Data owner has also the right to dispatch the data to any other Data owner by performing, if so applicable, any anonymization activities needed. Finally, the Data owner can view any analytics results that are relevant to a case.

2.3.1.2 Data processor

The Data processor is responsible for performing analytics and for normalizing the stored data. The analytics may concern data from past cases, or suggestions that are the output that the recommendation engine generates based on profile data, previous case data and social media data. Normalization of data in this context means the alignment of data of various cases by finding duplicates, categorizing data etc. The main responsibility of the Data processor is to ensure that there are no inconsistencies in the stored data and to configure the recommendation engine to obtain the best possible results

2.3.1.3 Data management

The Data management role has all the duties relevant to data maintenance. Operations like back-up, restore and archiving are the typical responsibilities of the Data management role. As the Data manager needs not know the contents of the database to perform the desired actions, extra security can be offered by performing anonymization to any piece of data that is stored in the organisation.

3 Legal framework

3.1 European legislation

Missing children successful investigation and rescue involves among other things the storage and processing of the minor's and his/her family personal data. The development of a mobile application that will engage several users, actors and authorities intends to accelerate the missing child's recovery. In this context, law concerning data protection and personal data processing shall be taken into consideration, in order for the ChildRescue application to be fully aligned with current international, European[15] and national legal provisions.

3.1.1 The right to private life and data protection

For the first time, a right to protection of an individual's private sphere against intrusion from others, especially from the state, was established in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life[16]. Thereafter European legal instruments have been influenced and established. The right to data protection evolved out of the right to respect for private life.

The European Convention on Human Rights

The Council of Europe, as it was formed in the aftermath of the Second World War, adopted the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights - ECHR)[17] in 1950, which entered into force in 1953[18]. ECHR sets forth a number of fundamental rights and freedoms (right to life, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security, right to a fair trial, no punishment without law, right to respect for private and family life, freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association, right to marry, right to an effective remedy, prohibition of discrimination). More rights are granted by additional protocols to the Convention. Noteworthy that, under the Lisbon Treaty, fundamental rights, as guaranteed by the ECHR and as they result from the constitutional traditions of the Member States, constitute the general principles of the Union's law[19].

[15] For the structure of the European legal framework, the European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2014, available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf has been also considered.

[16] United Nations (UN), Universal Declaration of Human Rights (UDHR), 10 December 1948, available at: http://www.un.org/en/universal-declaration-human-rights/index.html .

[17] CoE, European Convention on Human Rights, CETS No. 005, 1950, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005.

[18] States have an international obligation to comply with the ECHR and to this end, the European Court of Human Rights (ECtHR), was set up in 1959, where complaints from individuals, groups of individuals, NGOs or legal persons and States alleging violations of the Convention are received and considered to ensure the observance of the engagements undertaken by the Parties. To date, the Council of Europe comprises of 47 member states, out of which are 28 EU member states; https://www.coe.int/en/web/about-us/who-we-are

[19] Article 1 of the Lisbon Treaty amending article 6 para 3 of the Rome Treaty.

Under the ECHR the right to protection of personal data is guaranteed in Article 8 as part of the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted, such as when in accordance with law and in the interests of public security and public safety, for the prevention of disorder or crime, for the protection of rights and freedoms of others.

Council of Europe Convention 108

In need for the development of more detailed rules to safeguard individuals by protecting their personal data and following a series of resolutions that were adopted by the Committee of Ministers of the Council of Europe,[20] in 1981 the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[21] was opened for signature[22]. Convention 108 applies to all data processing carried out by both the private and public sector, here including the judiciary and law enforcement authorities and seeks to regulate the trans-border flow of personal data. It lays down principles for the collection and processing of personal data in order to protect the individual form abuses during these process, namely fair and lawful collection and automatic processing of data, storage for specified legitimate purposes (legitimacy) and for the time necessary and appropriate and use compatible with the legitimate purposes. Data processed shall be adequate, relevant, proportionate to the purpose and accurate (quality of data; proportionality). At the same time, 'sensitive data', such as a person's race, politics, health, religion, sexual life or criminal record are excluded from collection and processing, unless the necessary legal requirements are met. Moreover, under the Convention the individual has the right to be aware that information is stored on him or her and, if necessary, to react (transparency and free, specific and informed consent). Restrictions on the provided rights are possible only when overriding interests, such as state security or defence, are at risk.

In 2017 the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data issued the Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data[23]. These comprise of recommendations to state parties to the Convention, controllers and processors to undertake measures related to data protection for the prevention of potential negative impact of the use of Big

[20] Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 September 1973; CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector, 20 September 1974).

[21] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 . In 1999, Convention 108 was amended to enable the EU to become a Party (see Art. 23 (2) of the Convention 108 in its amended form). In 2001, an Additional Protocol to Convention 108 was adopted, introducing provisions on transborder data flows to non-parties (third countries) and on the mandatory establishment of national data protection supervisory authorities; available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181 . Note: Greece and Belgium have not ratified the Protocol.

[22] Up to date, all 47 members of the Council of Europe have ratified the Convention and 4 non-members of the CoE. Convention 108 is the only legally binding international instrument in the data protection field.

[23] Available at: https://rm.coe.int/16806ebe7a

Data[24] on human dignity, human rights and fundamental freedoms. The purpose is to limit the risks for data subjects' rights, such as the potential bias of data analysis, the underestimation of the legal, social and ethical implications of Big Data on decision-making processes (e.g. mere de-contextualised information being the grounds of a decision), and the marginalization of an effective and informed involvement by individuals in these processes (e.g. in case of power imbalance between controller and data subject). Finally, modernization proposals for the Convention 108 have been elaborated since 2013 transmitting a draft amending protocol in 2016, but it has not been finalised yet.

European Union data protection law

EU law is composed of primary EU law, namely Treaty on European Union (TEU)[25] and the Treaty on the Functioning of the European Union (TFEU - Lisbon Treaty)[26] and secondary EU law, i.e. regulations, directives and decisions of the EU.

The Charter of Fundamental Rights of the European Union

In 2000 the Charter of Fundamental Rights of the European Union (Charter)[27] was proclaimed[28] by the EU. Tough a political document at first, the Charter became legally binding as EU primary law with the coming into force of the Lisbon Treaty in 2009[29].

The rights enshrined in the Charter are divided into six sections: dignity, freedoms, equality, solidarity, citizens' rights and justice. The Charter guarantees the respect for private and family life[30], and explicitly raises the level of data protection to that of a fundamental right in EU law by establishing the right to data protection[31]. It refers to key data protection principles, such as fair processing and for specific purpose, individual's consent or based on other legal basis[32], and ensures that an independent authority will control the implementation of these principles[33].

3.1.2 General Data Protection Regulation

Under article 16 of the TFEU, where the right to protection of personal data is safeguarded, the competency of the European Parliament and the Council to legislate on data protection matters is

[24] Therein the term Big Data encompasses both Big Data and Big Data analytics. Big Data are identified as extremely data sets with heterogeneous characteristics that may be analysed computationally to extract inferences about data patterns, trends and correlations; Guidelines, p.2

[25] Consolidated version of the TEU available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT

[26] Consolidated version of the TFEU available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

[27] EU (2012), Charter of Fundamental Rights of the European Union, OJ 2012 C 326, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

[28] Namely, at that time, it was not incorporated into the Treaty and was not legally binding.

[29] All amendments available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12007L/TXT

[30] Art. 7: "Everyone has the right to respect for his or her private and family life, home and communications."

[31] Art. 8(1): "Everyone has the right to the protection of personal data concerning him or her."

[32] Art. 8(2): "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

[33] Article 8(3): "Compliance with these rules shall be subject to control by an independent authority."

foreseen[34]. The principal EU legal instrument on data protection is the Regulation (EU) 2016/279 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)[35]. By this Regulation, Directive 95/46/EC (Data Protection directive)[36] was repealed and GDPR comes into force on 25 May 2018. As stipulated in the recitals of the GDPR, while a high level of natural persons' protection must be ensured with regards to the personal data processing, this should be balanced against other fundamental rights in accordance with the principle of proportionality. The technological developments and the expansion of data processing and sharing made it imperative upon the Union bodies that a strong and more coherent data protection framework should be established. Thus, a homogenous application of law throughout the EU could only be established with an EU regulation[37].

Table 3-1 Key points

Key points[38]
Citizens' rights
The GDPR strengthens existing rights, provides for new rights and gives citizens more control over their personal data. These include: • **easier access to their data** — including providing more information on how that data is processed and ensuring that that information is available in a clear and understandable way; • **right to data portability** — making it easier to transmit personal data between service providers; • **right to erasure** ('right to be forgotten') — when an individual no longer wants their data processed and there is no legitimate reason to keep it, the data will be deleted; • **right to know when their personal data has been hacked** — companies and organisations will have to inform individuals promptly of serious data breaches. They will also have to notify the relevant data protection supervisory authority.
Rules for businesses
The GDPR is designed to create business opportunities and stimulate innovation through a number of steps including: • **a single set of EU-wide rules**; • **a data protection officer**, responsible for data protection, will be designated by

[34] TFEU, Art. 16(2), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

[35] General Data Protection Regulation, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1522240823531&from=EN

[36] Data Protection Directive, OJ 1995 L 281, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 .

[37] "Regulations are of general application, binding in their entirety and directly applicable. They must be complied with fully by those to whom they apply (private persons, Member States, Union institutions). Regulations are directly applicable in all the Member States as soon as they enter into force (on the date stipulated or, failing this, on the twentieth day following their publication in the Official Journal of the European Union) and do not need to be transposed into national law.

They are designed to ensure the uniform application of Union law in all the Member States. Regulations supersede national laws incompatible with their substantive provisions."; information retrieved from 'Sources and Scope of European Union Law', Fact sheets in the European Union - 2018, available at: http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.2.1.pdf

[38] Retrieved from: Protection of personal data, Regulation (EU) 2016/279, Summary of legislation, available at: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32016R0679&qid=1522240823531

public authorities and by businesses which process data on a large scale;

- **one-stop-shop** — businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
- **EU rules for non-EU companies** — companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;
- **innovation-friendly rules** — a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default);
- **privacy-friendly techniques** such as pseudonymisation (when identifying fields within a data record are replaced by one or more artificial identifiers) and encryption (when data is coded in such a way that only authorised parties can read it);
- **removal of notifications** — the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free flow of personal data within the EU. This will make it easier for businesses to expand;
- **impact assessments** — businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;
- **record-keeping** — SMEs[39] are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.

3.1.2.1 Definitions and scope

GDPR lays down rules for the protection of natural persons[40], irrespective their nationality or residence, regarding the processing of their personal data and rules relating to the free movement of personal data (Article 1). Particularly, it applies to the processing of personal data wholly or partly by automated means, as well as by other than automated means when the personal data form or are intended to form part of a filing systems (Article 2). Furthermore, with regard to the territorial scope of the GDPR[41], it applies to processing of personal data by an establishment[42] of a controller or a processor in the Union, whether a branch or a subsidiary with legal personality[43]; the processing of data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to offering goods or services to such data subjects, irrespective of payment[44]; the processing of personal data of data subjects who are in the Union by a

[39] Small and medium-sized enterprises

[40] And not deceased; Recital 27.

[41] Art. 3 GDPR

[42] According to Art. 4(16) of the GDPR, "'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;"

[43] Recital 22

[44] Recital 23

controller or processor not established in the Union, when it is related to the monitoring of the behaviour of such data subjects in so far this behaviour takes place within the Union[45].

Noteworthy that anonymous information, namely information that cannot be attributed to an identified or identifiable natural person or personal data that have become anonymous by making the data subject no longer identifiable, including for statistical or research purposes, are not regulated by the GDPR. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria do not fall within the scope of the GDPR[46]. Moreover, the processing of personal data by private individuals for merely personal or household purposes falls also out of the scope of this Regulation (household exemption)[47]. GDPR does not apply for the processing of the personal data by the Union institutions, bodies and offices and agencies, as this falls under the scope of Regulation (EC) 45/2001. In addition, with regard to processing by the judiciary and law enforcement authorities concerning the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, Directive (EU) 2016/680 applies.

Under article 4 of the GDPR,

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, particularly by reference to an identifier such as name, ID number, location data (e.g. GPS), online identifier via devices, applications, tools and protocols (e.g. cookies, IP address, radio frequency identification tag)[48] or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (para 1); Personal data which have undergone pseudonymisation and thus could be attributed to a natural person with the use of additional information, should be regarded as information of an identifiable person[49]. To ascertain that, objective factors should be taken into account, such as the costs and the time required for identification, as well as the available technology at the time of processing[50].

Through the use of modern technology traces might be left, which when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them[51].

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

[45] Recital 24
[46] Recital 15
[47] Recital 18
[48] See also recital 30
[49] Recital 2
[50] Ibid.
[51] Recital 30

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (para 2);

'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (para 4);

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (para 5);

'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (para 6);

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or national law, the controller or the specific criteria for its nomination may be provided for by Union or national law (para 7);

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (para 8);

'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or national law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing (para 9);

'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data (para 10);

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (para 11);

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (para 12);

'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural

person and which result from the analysis of a biological sample from the natural person in question (e.g. DNA or RNA analysis)[52] (para 13);

'biometric data' means personal data resulting from specific technical processing relating to the physical, physio- logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data (para 14);

'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status[53] (para 15);

3.1.2.2 Basic principles of processing personal data

Table 3-2 Basic principles of personal data (PD) processing – Article 5 GDPR

Basic principles of personal data (PD) processing – Article 5 GDPR
✓ **Lawfulness, fairness and transparency** – PD processed lawfully, fairly and in a transparent manner in relation to the data subject;
✓ **Purpose limitation** – PD collected for specific, concrete and legitimate purposes and any further process must be compatible with these purposes[54];
✓ **Data minimisation** – adequate, relevant and limited to what is necessary to the purposes for which they are processed
✓ **Accuracy** – ensure that PD are accurate and, where necessary, kept up to date; PD that are inaccurate shall be erased or rectified without delay
✓ **Storage limitation** – PD shall be kept in a form that permits the identification of the data subject solely for the time necessary for the purpose for which the PD are processed[55];
✓ **Integrity and confidentiality** – during processing security of PD, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, shall be ensured, by undertaking appropriate technical and organisational measures
✓ **Accountability** - The controller shall be responsible for, and be able to demonstrate

[52] See also recital 34 GDPR

[53] E.g. according to Recital 35 GDPR, "a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test".

[54] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (art. 5(b)). See also art. 89(1) GDPR.

[55] Personal data may be stored for longer periods only if they are intended to be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) subject to implementation of the appropriate technical and organizational measures in order to safeguard the rights of the data subject (Article 5 point (e)).

compliance with the aforementioned principles

The *principle of lawfulness* requires that personal data should be processed *on the basis of the consent of the data subject concerned* or *some other legitimate basis,* laid down by GDPR or other EU or national law[56] (article 6).

Other legitimate basis, according to article 6 points (b) – (f), includes:

- the necessity for compliance with the legal obligation to which the controller is subject[57];
- the necessity for the performance of a contract to which the data subject is party or as step prior to entering into a contract at the request of the data subject;
- the necessity for the protection of the vital interests of the data subject or of another natural person[58];
- the necessity according to the legitimate interests pursued by the controller or by a third party[59], unless the interests or fundamental rights of the data subject, especially where he/she is a child, which require protection of personal data, transcend[60].

Based on European Court of Human Rights case-law, the limiting of the fundamental right to protection of personal data must be strictly necessary[61]. 'Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation'[62]. Moreover, the means of processing, the categories of data processed and the duration of data storage shall be necessary for the purpose of the processing[63]. Proportionality requires that the disadvantages for not fully exercising the right to data protection do not override the advantages due to limiting the right, namely the limitation should be justified and accompanied by safeguard measures[64]. A prerequisite is that 'the measure is adequate to achieve the envisaged objective' and that only adequate and relevant personal data for the purposes of processing are collected and processed[65].

[56] Art. 6 GDPR.

[57] "This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing." Recital 45 GDPR

[58] This should take place principally only where the processing cannot be established on another legal basis; Recital 46 GDPR.

[59] "At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place"; Recital 47 GDPR. Under Recital 49 GDPR, processing of personal data, where this is strictly necessary and proportionate for the purposes of ensuring network and information security, corresponds to a legitimate interest of the data controller.

[60] "The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing"; Recital 47 GDPR

[61] European Data Protection Supervisor, Necessity & Proportionality, available at: https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Ibid.

The purposes for personal data processing should be compatible with the purposes for which the personal data were initially collected and thus common legal basis covers both cases[66]. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority that the controller holds, EU or national law shall determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Where the data subject has given consent or the processing is based on Union or national law and constitutes a necessary and proportionate measure in a democratic society to safeguard, particularly, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes[67]. Yet, further processing of personal data should be compatible with legal, professional or other binding obligation of secrecy[68].

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. However, appropriate safeguards should be in place, for example pseudonymisation. Specific provisions are foreseen under article 89 and these are thoroughly described in recitals 156-162.

The *principle of transparency* requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language or even visualisation be used[69], especially for information addressed to a child[70]. Information should be provided in writing or by other means, including electronic means. When information is provided orally, the identity of that data subject must proven by other means[71].

Accountability corresponds to the active implementation of measures by controllers to promote and safeguard data protection in their processing operations. Controllers are responsible for the compliance of their processing activities with the GDPR and should be able at any time to demonstrate compliance to the general public and to supervisory authorities[72].

Processing of special categories of personal data[73]

- Under Recitals 51-54 of the GDPR, it is highlighted that there are personal data which are particularly sensitive in relation to fundamental rights and freedoms and for this reason these require specific protection, as the context of their processing could create significant risks[74]. These data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data

[66] Recital 50(1)

[67] Recital 50(2)

[68] Recital 50(2).

[69] Art 13(1). Such information could be provided in writing or electronic form, for example, when addressed to the public, through a website; Recital 58.

[70] Recital 58

[71] Art. 12(1)

[72] See accordingly, European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2014, p. 75, available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

[73] Art. 9 and Recital 51-54

[74] See particularly Recital 51

concerning a natural person's sex life or sexual orientation[75]. Processing of such personal data should be prohibited, unless it meets concrete conditions, such as the following[76,77]:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes[78];

(b) processing is based on obligation and specific right of the controller or of the data subject in the field of employment and social security and social protection law and is established in EU or national law or a collective agreement pursuant to national law providing for appropriate safeguards for the fundamental rights and interests of the data subject[79];

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim within its legitimate activities and concerns solely the members or former members of the body or persons having regular contact with it in relation to its purposes and the personal data are not disclosed outside that body without data subjects' consent;

(e) processing concerns personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary on the basis of substantial public interest according to EU or national law, which shall be proportionate to the aim pursued, respect the right to data protection and provide for measures to safeguard the data subject's fundamental rights and interests;

(h) processing is necessary for health-related purposes for the benefit of natural purposes and society as a whole, such as medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or national law or pursuant to contract with a health professional who is bounded by professional secrecy[80];

(i) processing is necessary for reasons of public interest in the area of public health on the basis of EU or national law which provides for measures to secure the rights and freedoms of the data subject, particularly professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on EU

[75] Art. 9

[76] Art. 9(2)

[77] According to art. 9(4) of the GDPR, 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health'.

[78] except where EU or national law provide that the prohibition may not be lifted by the data subject; GDPR, Article 9(2) point (a)

[79] See also recital 52.

[80] See also art. 9(3) and recital 53.

or national law which shall be proportionate to the aim pursued, respect the right to data protection and provide for measures to safeguard the data subject's fundamental rights and interests.

- Processing of personal data concerning criminal convictions and offences or related security measures will only be possible when conducted under the control of a public authority or when this is based on EU or national law and appropriate safeguards are in place[81].

3.1.2.3 Consent

Consent, as examined above, is, in numerous cases, the legal basis for legitimate data processing. Consent must be free, informed, specific and unambiguous; it should be a clear affirmative act indicating the data subject's acceptance of the proposed processing of his/her personal data, in the form a written statement or an electronic form or an oral statement (e.g. ticking a box when visiting a website, choosing technical settings for information society services).[82]. Especially where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data[83]. Therefore, a declaration of consent pre-formulated by the controller should be provided in a comprehensible and easily accessible form, using clear and plain language and it should not contain unfair terms, ensuring that the data subject is aware and particularly of the extent to which consent is given[84]. In addition, in the case of a written declaration including other matters as well, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters'[85]. Any part that does comply with the GDPR rules is not binding[86].

For consent to be informed, the data subject should know at least the identity of the controller and the purposes of the processing[87]. At the same time, consent should not be regarded as freely given, not unless the data subject has genuine or free choice or is able to refuse or withdraw consent without detriment[88]. Data subject should be informed prior to giving his/her consent that he/she is able to withdraw at any time[89]; the procedure should be as easy as giving consent[90]. In addition, consent to be freely given requires that it allows separate consent to be given to different personal data processing operations[91]. Further, in case of contract performance or service provision, these must not be conditional on the consent for processing, if this is not a prerequisite for the performance of the contract or service[92]. Where there is clear imbalance between the controller and the data

[81] Art. 10.
[82] Recital 32.
[83] Art. 7(1); Recital 42
[84] Recital 42; see also Council Directive 93/13/EEC (1)
[85] Art. 7(2) GDPR
[86] Art. 7(2)
[87] Recital 43
[88] Recital 42
[89] Art. 7(3). Note: According to art.7(3), 'the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal'.
[90] Art. 7(3)
[91] Recital 43
[92] Art. 7(4); Recital 43

subject, it should be presumed that consent is not given freely and thus consent should be the legal basis for processing[93].

Under the GDPR, it is acknowledged that children should be granted specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards at stake, as well as their rights with regard to the processing of personal data[94]. This is especially apparent as concerns the field of marketing and information society services[95]. On that account, a child shall be at least 16 years old to consider the consent lawful[96]. For children below the age of 16 years, consent is given or authorised by the holder of parental responsibility over the child[97] and the controller should make reasonable efforts to verify that[98]. By contrast, in the context of preventive or counselling services offered directly to a child, the consent of the holder of parental responsibility should not be necessary[99].

3.1.2.4 Responsibilities of the controller, the processor & the data protection officer

Responsibility of the controller

The controller is responsible for the implementation of appropriate technical and organisational measures to secure and be able to demonstrate that processing is performed according with the GDPR by taking into account the context and purpose of processing as well as the impact that this might have on the rights and freedoms of natural persons[100]. These measures may include data protection policies[101] or the application of approved codes of conduct or certification mechanisms[102]. Where two or more controllers define together the purpose and means of the processing, they are joint controllers with concrete responsibilities to comply with the GDPR[103]. This arrangement should be available for the data subject too[104].

Where the controller delegates a processor to perform the processing of personal data and to act on behalf of the controller, the latter must use only processors providing sufficient guarantees to

[93] Recital 43

[94] Recital 38

[95] According to point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council, 'Information society service'[95] means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request; Art.4(25) GDPR. Examples are: web shops and marketplaces, search engines, online advertising, video sharing sites, blogs, hosting, video-on-demand, online consultancy, online marketplaces, social networking, etc.

[96] Art. 8(1)

[97] Ibid.

[98] Art. 8(2)

[99] Recital 38

[100] article 24, para 1.

[101] Art. 24 para 2.

[102] Art. 24(3). See also articles 40 & 42 GDPR.

[103] Art. 26(1).

[104] Art. 26(2).

implement suitable technical and organisational measures in compliance with the GDPR and with respect to the data subject's rights[105].

Each controller, or representative of a controller in the EU, with regard to enterprises or organisation employing more that 250 persons, is responsible for keeping a record of the processing operations, in writing including in electronic form[106]. This record shall be available upon request of the supervisory authority[107]. The obligation to keep a record applies to organisations with less than 250 employees, where processing is likely to result in a risk to the data subject's rights, the processing is not occasional, or it includes personal data revealing sensitive information about an individual or relate to criminal convictions[108].

The controller is anticipated to cooperated with the supervisory authority upon request[109]. Nevertheless, in case of a personal data breach, the controller has to notify the supervisory authority within 72 hours after having become aware of the breach, expect for breaches that are unlikely to result in a risk to the data subject's rights[110]. If the notification takes place later than 72 hours, the reasons for this must be made known[111]. In the notification 'the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned' should be described; 'the name and contact details of the data protection officer or other contact point where more information can be obtained' should be communicated; 'the likely consequences of the personal data breach' should be described; as well as 'the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects' should be described[112]. The controller is responsible for documenting any personal data breaches (facts relating to the breach, effects and remedial measures taken) in order for the supervisory authority to verify compliance with GDPR provisions[113].

The controller is responsible for communicating a personal data breach to the data subject, using a clear and plain language, if it is likely to affect negatively the natural person's rights[114]. If measures have been taken, such as encryption or other, that either render personal data intelligible or the risk no longer exists, the controller does not have to inform the data subject[115]. In case, it demands disproportionate effort to reach the data subject(s) affected, then public communication or similar measure should be employed[116].

[105] Art. 28(1).
[106] Art. 30 paras 1,3,5.
[107] Art. 30(4).
[108] See articles 9(1) & 10.
[109] Art. 31.
[110] Art. 33(1).
[111] Ibid.
[112] Art. 33(3).
[113] Art. 33(5).
[114] Art. 34 paras 1-2.
[115] Art. 34(3).
[116] Ibid.

The controller is liable for any damage caused by a processing that violated the GDPR[117], unless the controller proves that it is not responsible for the cause of the damage[118].

Responsibility of the processor

The processor must be bound by a contract or other legal act under EU or national law with regard to the controller and act in accordance as to the processing operations[119]. Therein 'the subject-matter and duration of processing, the nature and purpose of processing, the type of personal data and categories of data subjects and the obligation and rights of the controller' are set out[120]. Under article 28 para 3 of the GDPR specific clauses to be part of the contract or legal act are foreseen, such as that (a) the processing takes place only under documented instructions by the controller unless the processor is obliged to act so by EU or national law; (b) the processor ensures that authorised persons to process personal data are bound by confidentiality obligation; (c) the processor takes all necessary technical and organisation measures to secure the protection of data subject's personal data; (d) the processor cannot engage other processors unless there is a prior written authorisation of the controller[121] - in case the authorisation is general, the processor has to inform the controller for any intended changes regarding the engaged processors[122]; (d) the processor assist the controller to respond to requests by data subjects exercising their rights under the GDPR; (e) the processor, if requested so by the controller, shall delete or return all personal data to the controller by the end of the provision of services and delete copies unless obliged otherwise by EU or national law; (f) processor provides necessary information to the controller for the latter to establish compliance of the first with the obligation laid down in article 28 GDPR and contribute to audits and inspections conducted by the controller[123]. If, to processor's opinion, a controller's instruction infringes the GDPR, the processor must immediately inform the controller[124]. Standard contractual clauses for the aforementioned matters may be laid down by the European Commission or the supervisory authority[125]. In any event, the contract or other legal act must be in writing, including in electronic form[126].

If the processor engages another processor to perform specific processing activities on behalf of the controller, the same data protection obligations must be stipulated in a similar contract or other legal act[127]. Where that processor does not fulfil its data protection obligations, the initial processor remains fully liable to the controller for the acts of the other processor[128]. Sufficient guarantees of implementing appropriate technical and organisational measures in a manner that processing meets

[117] Art. 82(2).
[118] Art. 82(3).
[119] Art. 28(3).
[120] Ibid.
[121] Art. 28(2).
[122] Ibid.
[123] See also article 28(3), point (f) & article 32: "security of processing".
[124] Art. 28(3).
[125] Art. 28 paras 6-8.
[126] Art. 28(9).
[127] Art. 28(4).
[128] Ibid.

the requirements of the GDPR may be demonstrated by the adherence of the processor to an approved code of conduct or certification mechanism[129]. The processor or any person acting under the authority of the controller or the processor, shall process personal data only on the instructions of the controller or the processor, unless EU or national law defines otherwise[130].

Each processor or the representative of a processor in the EU is responsible for keeping a record of all categories of processing operations performed on behalf of the controller, in writing including in electronic form[131]. This record shall be available for the supervisory authority upon request. The same criteria for the obligation to keep record in relation to the size of an enterprise or organisation, as with the controller, apply[132]. In any event, the processor is anticipated to cooperated with the supervisory authority, upon request[133].

The processor as soon as becomes aware of a personal data breach must notify the controller[134].

A processor is liable for damage resulting from a processing only where he has acted contrary to or outside the obligations under the GDPR or the lawful instructions of the controller[135]. The processor is exempted from liability, if it proves that it is not responsible for the cause of the damage[136].

The role of the data protection officer

A data protection officer (DPO) must be designated by the controller or the processor, if: (a) processing is carried out by public authority or body, (b) in the context of the processing, regular and systematic monitoring of data subjects on a large scale takes place, (c) large scale processing of personal data revealing sensitive information about individuals or criminal convictions takes place[137]. Apart from the aforementioned cases, the controller or processor should designate a data protection officer, where required by EU or national law[138]. One data protection officer may serve more controllers or processors[139]. He/she must have expert knowledge of data protection law and practices and the ability to carry out tasks provided under the GDPR[140]. He/she may be a staff member of the controller or processor, or be engaged by a service contract[141]. Contact details of the DPO shall be published and communicated to the supervisory authority too.[142]

[129] Art. 28(5).
[130] Art. 29.
[131] Art. 30 paras 2& 4.
[132] GDPR article 30 para 5.
[133] Article 31 GDPR.
[134] GDPR Article 33 para 2.
[135] GDPR article 82 para 2.
[136] GDPR article 82 para 3.
[137] GDPR article 37 para 1.
[138] GDPR article 37 para 4.
[139] GDPR article 37 paras 2-3.
[140] GDPR article 37 para 5.
[141] GDPR article 37 para 6.
[142] GDPR article 37 para 7.

DPO shall be involved in all issues concerning the protection of personal data[143] and shall directly report to the highest management level of the controller or processor[144]. The controller and processor support the DPO in carrying out his/her tasks under the GDPR (resources, access to personal data processing activities, continuous training)[145] and do not instruct him/her[146]. However, the controller or processor shall make sure that there is no conflict of interest, if the DPO is engaged in several positions[147]. In any event, DPO must be bound by secrecy or confidentiality with regard to his/her tasks[148]. Finally, DPO should be available for data subjects to contact him/her in relation to their personal data[149].

Under article 39 para 1 of the GDPR the DPO is assigned with specific tasks, namely (a) 'to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to' the GDPR and to other EU or national data protection provisions; (b) 'to monitor compliance with' the GDPR, with other EU or national 'data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits'; (c) 'to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35' of the GDPR; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36' of the GDPR, 'and to consult, where appropriate, with regard to any other matter'.

During the performance of his/her tasks, the DPO has to take into consideration the risks deriving from processing activities, including the nature, scope, context and purposes of processing[150].

3.1.2.5 Data protection safeguards

- *Information to be provided, where personal data have been collected from the data subject*

As soon as personal data are obtained from the data subject and insofar as the data subject is not already aware of, the controller has to provide certain pieces of information, such as (a) the identity and contact details of the controller or the controller's representative[151], (b) the contact details of the data protection officer where applicable, (c) the purpose of the personal data processing and the legal basis for it, (d) if processing is based on the legitimate interest of the controller, then these should be made known (e) the recipients of the personal data, if any (f) where applicable, the

[143] GDPR article 38 para 1.
[144] GDPR article 38 para 3.
[145] GDPR article 38 para 2.
[146] GDPR article 38 para 3.
[147] GDPR article 38 para 6.
[148] GDPR article 38 para 5.
[149] GDPR article 38 para 4.
[150] GDPR article 39 para 2.
[151] 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation; Article 4 (17) GDPR.

intention to transfer of data[152]. Apart from the aforementioned, the controller shall provide further information about (a) the time period of data storage, (b) the existence of the right to request access to and rectification or erasure of personal data or restriction of processing, as regards the data subject's personal data or to object to processing as well as the right to data portability, (c) when processing is based on the data subject's consent, the right to withdraw consent at any time, without affecting the lawfulness of processing before its withdrawal, (d) the right to lodge a complaint with a supervisory authority, (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of not providing them, (f) the existence of automated decision-making, including profiling, the logic involved and the significance or potential consequences of such processing for the data subject[153]. Lastly, if the controller intends to proceed with further processing of the data subject's personal data for a purpose different from the one for which the data where initially collected, then the data subject must receive all relevant information[154].

- *Information to be provided, where personal data have not been collected from the data subject*

  In case the personal data have not been obtained from the data subject and the latter is not already aware of, the controller has the same obligation to inform the data subject within a reasonable period after obtaining the personal data, but at least within a month or if applicable in the first communication with the data subject or if applicable in the first disclosure of the data to another recipient[155]. In addition to the previously mentioned, the controller has to further inform the data subject about the categories of personal data concerned[156] and the sources from which the data originate and whether these publicly accessible sources[157]. Information should be provided free of charge[158]. These is no obligation for the controller to inform the data subject, if this proves impossible or involves disproportionate effort or it might not serve the objectives of the processing[159]. Making information publically available could balance both sides interests[160]. Moreover, where obtaining or disclosure is directly provided in EU or national law taking into account the necessary rights protection safeguards or where data must remain confidential (statutory obligation of secrecy), the controller shall not provide any information to the data subject[161].

- *Data protection by design and by default*

[152] Article 13 (1), (4) GDPR.
[153] Article 13(2) GDPR.
[154] Article 13(3) GDPR.
[155] Article 14 (1)-(4) GDPR.
[156] Article 14(1), point (d) GDPR.
[157] Article 14(2), point (f) GDPR.
[158] Article 12(5) GDPR.
[159] Article 14(5), point (b) GDPR.
[160] In this case the legislator suggests that appropriate measures should be taken to protect the data subject's rights and interests, including making the information publically available; Article 14(5)b GDPR.
[161] Article 14(5), points (c)-(d) GDPR.

By design of the processing and implementation of it, the controller has to apply technical and organisational measures for safeguarding data protection principles effectively[162]. Moreover, by default, the amount of personal data collected, the extent of their processing, the period of storage and their accessibility must be regulated in a manner that all principles are ensured[163].

- *Security of processing*

The controller and processor have to take all necessary technical and organisation measures to ensure data protection and prohibit personal data breaches or any other potential risks for the rights and freedoms of natural persons[164]. Pseudonymisation and encryption are introduced as measures which could be applied to reduce these risks[165]. In the case of psedonymisation, it is stipulated that additional information which could render a natural person identifiable should be kept separately[166]. Furthermore, to ensure a level of security against such risks, measures that safeguard the ongoing confidentiality, integrity, availability and resilience of processing systems and services, or that restore the availability and access to personal data in a timely manner in the event of a physical or technical incident shall be implemented. Therein, the establishment of a process for regularly testing, assessing and evaluating the effectiveness of the security measures is provided. Additional safeguards can be adherence to an approved code of conduct[167] or an approved certification mechanism[168]. At any event, in assessing the security level, risks to be considered should be the ones deriving 'from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'[169]. Moreover, precautions must be taken for natural persons acting under the authority of the controller or the processor who have access to personal data to process them only on instructions from the controller or according to EU or national law[170].

- *Codes of conduct*

Codes of conduct are encouraged to be drafted to contribute to the proper application of the GDPR by the Member States, the supervisory authorities[171], the European Data Protection Board[172] and the European Commission[173]. 'Associations and other bodies representing categories of controllers or processors may prepare codes of conduct or amend or extend such codes' to specify the application of the GDPR, with regard to the particular features of the processing operation and principles for data protection and processing (e.g. fair and transparent processing, legitimate interest of the controller, collection of personal data, pseudinymisation, information provision to data subjects)[174]. The

[162] GDPR, article 25, para 1.
[163] GDPR, article 25, para 2.
[164] See for example recital 28 GDPR; articles 25 & 32 GDPR.
[165] Article 32 para 1 & recital 28 GDPR.
[166] Ibid.
[167] See article 40 GDPR.
[168] See article 42 GDPR.
[169] GDPR, article 32 para 2.
[170] GDPR, article 32 para 4.
[171] See articles 51-59 GDPR.
[172] See articles 68-76 GDPR.
[173] GDPR, article 40, para 1.
[174] GDPR, article 40 para 2.

monitoring of compliance with a code of conduct, as foreseen in article 41 GDPR, 'may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

- *Processing which does not require identification*

In case the controller is not able to identify a data subject from the personal data processed, then the controller should not be obliged to obtain additional information in order to identify the data subject, unless this is offered by the data subject in order to help the latter exercise his/her rights. In such a case, an authentication mechanism could be applied as a digital identification of the data subject (e.g. logging in to the online service)[175].

- *Data protection impact assessment and prior consultation*

When there is the likelihood that a type of processing, particularly by the use of new technologies, could result in a high risk to the rights of natural persons, the controller should conduct beforehand an assessment of the impact of the intended processing operations on the protection of personal data[176]. This would be particularly required in case of (a) systematic and extensive evaluation of personal aspects of natural persons, based on automated processing, including profiling, and which further becomes grounds for decisions that produce legal effects for the natural person or significantly affect him/her, (b) processing on a large scale of special categories of data revealing sensitive information about a natural person[177], or of personal data relating to criminal convictions and offences[178]; (c) a systematic monitoring of a publicly accessible area on a large scale[179]. Similar processing operations that present the same high risk could be addressed with one single assessment[180]. Such processing occasions should be listed by the supervisory authority, as well as those cases where no impact assessment is necessary[181]. Where processing is based on EU or Members State law under specific clauses[182] to which the controller is subject, a data protection impact assessment has already been carried out in the context of the adoption of that legal basis[183].

Under article 35 para 7 of the GDPR, the minimum content of an assessment is provided. In accordance, the assessment should contain at least: (a) a systematic description of the anticipated processing operations and its purposes, including, where applicable, the legitimate interest pursued by the controller, (b) an assessment of the necessity and proportionality of the processing in relation to the purposes, (c) an assessment of the risks to the rights and freedoms of data subjects, and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR

[175] Recital 57 GDPR.
[176] GDPR, article 35, para 1.
[177] See also article 9(1) GDPR.
[178] See also article 10 GDPR.
[179] GDPR, article 35, para 7.
[180] GDPR, article 35, para 1.
[181] GDPR, article 35, paras 4-5.
[182] See GDPR, article 6 para 1, point (c) or (e).
[183] GDPR, article 35 para 10.

taking into account the rights and legitimate interests of data subjects and other persons concerned. Compliance with approved codes of conduct will be taken into account for the assessment[184].

Where a data protection impact assessment indicates that the processing would result in a high risk, if no measures are taken by the controller to mitigate the risk, the controller must consult the supervisory authority prior to processing[185].

3.1.2.6 Data subject's rights

GDPR provides for the rights of the data subject in relation to the processing of his/her personal data. The controller should facilitate the exercise of the data subject's rights by providing modalities, such as easy accessible and free of charge mechanisms to make the request[186].

Right of access by the data subject[187]

The data subject holds the right to receive a confirmation as to whether or not his/her personal data are being processed and where that is the case to information such as the purpose of processing, the categories of personal data in question, the recipients that the data have been or will be disclosed, the existence of the right of rectification or erasure of personal data or restriction of processing or the right to object to the processing, the right to lodge a complaint; the sources from which the controller collected the data, the existences of automated decision-making. Moreover, the controller shall provide a copy of the personal data being processed[188]. Importantly, the controller should verify the identity of a data subject prior to giving access[189].

Right to rectification[190]

The data subject has the right to demand from the controller to correct inaccurate personal data. If data are incomplete, the data subject has the right to have them completed.

Right to erasure ('right to be forgotten')[191]

Under certain conditions, the data subject has the right to demand from the controller the erasure of personal data without undue delay. These conditions are limited to the following[192]:

> (a) the necessity principle is no longer satisfied in relation to the purposes for which the personal data were initially collected or processed;

[184] GDPR, article 35, para 8.
[185] See article 36 GDPR.
[186] See recital 59 GDPR.
[187] Article 15 GDPR.
[188] See also Recital 63 GDPR.
[189] Recital 64 GDPR.
[190] Article 16 GDPR.
[191] Article 17 GDPR.
[192] GDPR, article 1, para 1.

(b) where consent was the only legal basis for personal data processing and the data subject withdraws consent;

(c) the data subject objects to the processing in the context of controller's task performance in the public interest or on controller's legitimate interests and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for marketing purposes;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in EU or national law to which the controller is subject;

(f) the personal data have been collected from a person below 18 years of age in the context of information society services[193].

In case of personal data made public by the controller and the latter is obliged to erase the personal data, the controller has to take all reasonable measures to inform controllers processing these personal data too, that the data subject has requested erasure 'of any links to or copy or replication of those personal data'[194].

However, the right to erasure is balanced with other rights, legal obligations or reasons and, to the extent that processing is necessary for respecting these, can only partly apply[195]. Such cases are the right to freedom of expression and information, the legal obligation to comply with EU or national law or the exercise of official authority of the performance of a task in the public interest where in all previous occasions processing is required, the public interest for public-health related reasons, archiving purposes in the public interest, 'scientific or historical research purposes or statistical purposes in accordance with Article 89(1)' GDPR 'in so far as reassure of personal data is likely to render impossible or seriously impair the achievement of the objectives of that processing' and the right to exercise and defend a legal claim[196].

Right to restriction of processing

In terms of provisional protection, the data subject has the right to obtain from the controller restriction of processing[197] under specific circumstances, which are: when the accuracy of personal data is contested by the data subject (for necessary time to the controller to verify the accuracy); the processing is unlawful and the data subject's requests restriction of processing and not erasure of the personal data; the personal data are no longer necessary for the purposes of processing, but the data subject needs them to establish, exercise or defend legal claims; the data subject has objected to the

[193] For example, if a person had given his/her consent as a child and was not aware of the risks deriving from the processing, and later on, as an adult, desires to remove his/her personal data especially from the internet; recital 65 GDPR.

[194] GDPR, article 17, para 2.

[195] GDPR, article 17, para 3.

[196] Ib

[197] S

The controller shall notify all recipients of personal data in case of correction or erasure of personal data or restriction of their processing, unless this proves impossible or demands disproportionate efforts (article 19 GDPR).

legitimate interests of the controller and claims are examined[198]. In these cases, personal data cannot be processed unless with the data subject's consent or for the purpose of establishing, exercising or defending legal claims or for protecting the rights of another natural or legal person of for reasons of important public interest of the EU or of a Member State[199]. If restriction is about to be lifted, the controller must inform the data subject beforehand[200].

Right to data portability

Where processing of personal data is based on the data subject's consent and this is conducted through automated means, the data subject has the right to receive his/her personal data from the controller who was provide with the data, 'in a structured, commonly used and machine-readable format' and transmit those data to another controller[201]. This right does not apply 'to processing necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller'[202] or when it significantly impacts the rights and freedoms of others[203].

Right to object

Under certain conditions, the data subject has the right to object at any time to the processing of his/her personal data, which was grounded on the performance of tasks in the public interest or on the legitimate interests of the controller[204]. Unless the controller demonstrates that there are interests overriding the data subject's rights or that processing is necessary for the exercise of legal claims, the controller shall no longer process the personal data[205]. Until the first communication with the data subject, the controller must inform the data subject about this right explicitly[206]. Furthermore, 'where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest'[207].

Right not to be subject to a decision based solely on automated processing

The data subject has the right not to be subjected to a decision which is based on the evaluation of personal aspects that have been automatically processed, namely profiling, and which has legal effects upon him/her or significantly affects him/her[208]. The right is not applicable in case such a

[198] GDPR, article 18, para 1.
[199] GDPR, article 18, para 2.
[200] GDPR, article 18, para 3.
[201] GDPR, article 20, para 1. See also Recital 68 GDPR.
[202] GDPR, article 20, para 3.
[203] GDPR, article 20, para 4.
[204] GDPR, article 21, para 1.
[205] Ibid. Paras 2 & 3 concern processing for marketing purposes, which the data subject unconditionally can object to (see also recital 70 GDPR).
[206] GDPR, article 21, para 4.
[207] GDPR, article 21, para 6.
[208] GDPR, article 22, para 1.

decision is (a) necessary for entering into, or the performance of a contract between the controller and the data subject, (b) is authorised by EU or national law and the controller adheres to it (e.g. fraud and tax-evasion monitoring) and which foresees appropriate safeguards for the data subject's rights, (c) is based on the data subject's explicit consent[209]. Under (a) and (c) occasions, the controller has to provide suitable measures to ensure the data subject's rights and interest, such as 'the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'[210]. Such measure cannot involve a child data subject[211].

- The controller must provide information on action taken upon the request of the data subject under articles 15-22 of the GDPR without undue delay and in any event within one month from the receipt of the request[212].

Restrictions

Restrictions to the rights of the data subject and corresponding obligations of the controller may be imposed by EU or national law, as long as these respect fundamental rights and freedoms and is a necessary and proportionate measure to safeguard: national security; defence; pubic security; operations related to criminal offences or the execution of criminal penalties; other significant objectives of public interest of the EU or of a Member State; the protection of judicial independence and judicial proceedings; the prevention/investigation/detection/prosecution of breaches of ethics for regulated professions; monitoring, inspection or regulatory function related to the exercise of official authority; the protection of rights and freedoms of the data subject or others; the enforcement if civil law claims (GDPR, article 23, para 1). Such legislative measure shall contain minimum specific provision as stipulated under para 2 of the article 23 GDPR.

Right to remedy

Every data subject has the right to lodge a complaint before the competent supervisory authority[213]. In case the supervisory authority does not handle the complaint or does not inform the subject within three months on the progress or outcome of the complaint, the data subject has the right to an effective judicial remedy[214]. Furthermore, every natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority that concerns them[215]. The data subject, who considers that his/her rights under the GDPR have been violated by the controller due to processing in non-compliance with the GDPR, has, in addition, the right to an effective judicial remedy (directly)[216]. In case controllers were two or more, the data subject may exercise his/her rights under the GDPR against each of the controllers[217]. If such an infringement of

[209] GDPR, article 22, para 2. See also recital 71 GDPR.
[210] GDPR, article 22, para 3.
[211] Recital 71, GDPR.
[212] The time period may be extended if necessary and the controller has to inform the data subject for any extension; GDPR, article 12 para 3.
[213] Article 77 GDPR.
[214] GDPR, article 78, para 2.
[215] GDPR, article 78, para 2.
[216] Article 79 GDPR.
[217] GDPR, Article 26 para 3.

the GDPR has caused material or non-material damages to a person, then the controller or the processor have to compensate the person[218].

3.1.3 Other specific European data protection law

More specific provisions have been laid down with regard to the processing of personal data by police and criminal justice authorities, as well as the electronic communications.

Data protection law in the context of the police and criminal justice

In order to balance the individual's interests in data protection and society's interests in data collection for the purpose of fighting crime and ensuring national and public safety, a specific legal instrument was adopted together with the General Data Protection Regulation, namely the Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data ('Police Directive')[219]. This Directive has repealed the Council Framework Decision 2008/977/JHA, as to align with the provisions of the GDPR. Given that directives are not directly applicable, in order to come into force, they need to be transposed into national law. Therefore, national legislator must adopt a transposing act or other 'national implementing measure' to bring national law into line with the directive's objectives. EU countries have to incorporate the Police Directive into their national law by 6 May 2018.

Table 3-3 Key points

Key points[220]
The directive requires that the data collected by law enforcement authorities are: • processed lawfully and fairly; • collected for specified, explicit and legitimate purposes and processed only in line with these purposes; • adequate, relevant and not excessive in relation to the purpose in which they are processed; • accurate and updated where necessary; • kept in a form which allows identification of the individual for no longer than is

[218] Article 83 GDPR.

[219] Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&qid=1522240823531&from=EN

[220] Retrieved from: Protection of personal data, Directive (EU) 2016/680, Summary of legislation, available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG

necessary for the purpose of the processing; • appropriately secured, including protection against unauthorised or unlawful processing.
Time limits EU Member States must establish time limits for erasing the personal data or for a regular review of the need to store such data.
Individuals concerned ('data subjects') The directive requires that the law enforcement authorities make a clear distinction between the data of different categories of persons including: • those for whom there are serious grounds to believe they have committed or are about to commit a criminal offence; • those who have been convicted of a criminal offence; • victims of criminal offences or persons whom it is reasonably believed could be victims of criminal offences; • those who are parties to a criminal offence, including potential witnesses.
Information available or provided to data subject Individuals have the right to have certain information made available to them by the law enforcement (i.e. data protection) authorities including: • the name and contact details of the competent authority which decides the purpose and means of the data processing; • why their data is being processed; • the right to launch a complaint with a supervisory authority and the contact details of the authority; • the existence of the right to request access to and correction or deletion of their personal data as well as the right to restrict processing of their personal data.
Security National authorities must take technical and organisational measures to ensure a level of security for personal data that is appropriate to the risk. Where data processing is automated, a number of measures must be put in place, including: • denying unauthorised persons access to equipment used for processing; • preventing the unauthorised reading, copying, changing or removal of data media; preventing the unauthorised input of personal data and the unauthorised viewing,

changing or deleting of stored personal data.

The Police Directive aims at the enhanced protection of individuals' personal data, irrespective of their nationality or place of residence, when their data are processed by the police and criminal justice authorities and at the same time, at the improvement of cooperation in the fight against terrorism and cross-border crime within the EU by enabling police and criminal justice authorities in Member States to exchange information necessary for investigations more efficiently and effectively[221]. In particular, as articulated in recital 11 of the Directive, it regulates 'the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities'. An important aspect is that such competent authorities may be public, namely judicial authorities, the police or other law-enforcement authorities, but also private bodies or entities that have been assigned by national law to exercise public authority and public powers for the purposes of the Police Directive, i.e. the fight against crime. Therefore, 'a body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive'[222]. Moreover, this directive lays down the rules for the transfer of personal data for purposes that fall within the scope of the directive, such as from a member state to Interpol[223].

Member states are directed, to the extent feasible, to make a clear distinction between different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses, informants or associates of suspects and convicted criminals[224]. At the same time, this should not prevent the application of the right of presumption of innocence[225]. States should also distinguish verified and accurate data from personal data based on personal assessments[226]. Inaccurate data should not be made available or transmitted[227]. Moreover, states are directed expressly to establish appropriate time limits for deleting personal data or for a periodic review of the need for the storage of personal data and set a procedure to monitor whether time limits are respected[228].

[221] See also European Commission - Directorate General for Justice and Consumers, *How will the data protection reform fight international crime?*, factsheet January 2016, available at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41527
[222] Recital 11, Police Directive.
[223] Recital 25, Police Directive.
[224] Article 6 & Recital 31, Police Directive
[225] Recital 31, Police Directive.
[226] Article 7(1), Police Directive.
[227] Article 7(2), Police Directive.
[228] Article 5, Police Directive.

The principles for processing personal data, the role of controller, processor and data protection officer, as well as the rights of the data subject, as articulated in the Directive, are in alignment with the provisions of the GDPR. Yet, specific rules are further established to secure potential breaches of personal data that may adversely affect the data subject's fundamental rights and freedoms and to set limitations to the data subject's rights. Controller and processor should keep a record of all processing operations[229]. In addition, considering the nature, scope, context and purposes of the processing of personal data under this Directive, and the necessity for cross-border transfer of personal data in the fight against crime, concrete safeguards and conditions are set out.

Data protection in the electronic communications sector

Given that public communication services, such as the internet, mobile and landline telephony and their accompanying networks, information is exchanged and this may involve great interference to the individual's private life, specific rules and safeguards were necessary to ensure the users' right to privacy and confidentiality. European law in relation to data protection and electronic communications networks and services consists of the Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*)[230] as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009[231].

The Directive concerns the use of communication services in public electronic networks (internet & mobile phone networks) and sets out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications. It also bans unsolicited communications where the users have not given their consent. The Directive covers the communications of both natural and legal persons.

Table 3-4 Key points

Key points[232]

[229] Articles 24 & 25, Police directive

[230] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (*Directive on privacy and electronic communications*), OJ 2002 L 201. The consolidated version of the directive is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219 . 'This directive is one of five which together form the telecoms package, a legislative framework governing the electronic communications sector. The other directives cover the general framework, access and interconnection, authorisation and licensing and universal service. The package was amended in 2009 by two directives on better law-making and citizens' rights as well as by a regulation establishing the Body of European regulators for electronic communications.' For more information, see the European Commission's ePrivacy directive website.

[231] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136

[232] Retrieved from: Data protection in the electronic communications sector, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

Providers of electronic communication services must secure their services by at least: • ensuring personal data are accessed by authorised persons only; • protecting personal data from being destroyed, lost or accidentally altered and from other unlawful or unauthorised forms of processing; • ensuring the implementation of a security policy on the processing of personal data.
The service provider must inform the national authority of any personal data breach within 24 hours. If the personal data or privacy of a user is likely to be harmed, they must also be informed unless specifically identified technological measures have been taken to protect the data.
EU countries must ensure the confidentiality of communications made over public networks, in particular they must: • prohibit the listening, tapping, storage or any type of surveillance or interception of communications and traffic data without the consent of users, except if the person is legally authorised and in compliance with specific requirements; • guarantee that the storing of information or the access to information stored on user's personal equipment is only permitted if the user has been clearly and fully informed, among other things, of the purpose and been given the right of refusal.
When traffic data are no longer required for communication or billing, they must be erased or made anonymous. However, service providers may process these data for marketing purposes for as long as the users concerned give their consent. This consent may be withdrawn at any time.
User consent is also required in a number of other situations, including: • before unsolicited communications (spam) can be sent to them. This also applies to short message services (SMSs) and other electronic messaging systems; • before information (cookies) is stored on their computers or devices or before access to that information is obtained - the user must be given clear and full information, among other things, on the purpose of the storage or access; • before telephone numbers, e-mail addresses or postal addresses can appear in public directories.
EU countries are required to have a system of penalties including legal sanctions for infringements of the directive.

communications sector (Directive on privacy and electronic communications), available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:02002L0058-20091219

The scope of the rights and obligations can only be restricted by national legislative measures when such restrictions are necessary and proportionate to safeguard specific public interests, such as to allow criminal investigations or to safeguard national security, defence or public security.

Definitions

According to article 3 of the E-privacy Directive,

'user' means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof; traffic data may include 'data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network'[233].

'location data' means the data indicating the geographic position (latitude, longitude, altitude) of the terminal equipment of a user of a publicly available electronic communications service (e.g. direction to travel, identification of the network cell, in which the terminal equipment is located at a certain point in time and to the time the location information was recorded)[234];

'communication' means any information exchanged or conveyed between a restricted number of parties by means of a public electronic communications service. 'This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information'[235]; 'a communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication'[236].

Main provisions[237]

The provider of a public electronic communications service must take appropriate technical and organisational measures to guarantee security of its services, such as restricted access - authorised

[233] Recital 15.

[234] Recital 14.

[235] See also recital 16.

[236] Recital 15.

[237] See also European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2014, pp. 166-170, available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

persons, for legally authorized purposes, protection against personal data breaches[238], implementation of security policy, if necessary together with the provider of the public communications network with respect to network security[239].

Three main data categories generated during communication are identified and regulated in the e-privacy directive, namely the content of a communication, the traffic data and the location data. Confidentiality of electronic communications concerns not only the content of a communication (what was said or sent) but also to traffic data, such as information about who communicated with whom, when and for how long, and location data, such as from where data were communicated[240]. Traffic data have to be erased or made anonymous when they are no longer needed for the purpose of a communication transmission, unless the user has provided consent after being comprehensively informed about transmitting the data to added value service providers[241] (e.g. what is near my location-restaurants, bus station etc. or directions[242]) or for the improvements to the service provision. Location data can be processed only when they are made anonymous or with the specific and informed consent of the user[243]. Calling line identification (caller identification) and location data may be disclosed in cases of emergency[244]. Surveillance or interception of communications, for example, by listening or tapping devices, is prohibited unless it is provided for by law and constitutes a necessary measure in a democratic society in the interest of: protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences; or protecting the data subject or the rights and freedoms of others[245].

Furthermore, processing or transmission of data solely for marketing is fairly restricted to the cases where consent is provided[246], the user holds the right to be informed about the traffic data that are being kept and processed. In case a data breach occurs, as a result of unauthorised access, loss or destruction of data, the competent supervisory authority must be notified immediately[247]. Users must be informed if possible damage to them is the consequence of a data breach[248]. The establishment of judicial remedies is also foreseen[249].

[238] Under article 2, personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data trans- mitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community

[239] Article 4 para 1.

[240] Article 5.

[241] Article 6.

[242] See Recital 35.

[243] Article 9.

[244] Articles 8 & 10(2) & Recital 36.

[245] Articles 5(1) & 15(1). See also European Union Agency for Fundamental Rights (FRA), Handbook on European data protection law, 2014, p.170, available at: http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf

[246] Article 5.

[247] Article 4(3).

[248] Ibid.

[249] Article 15(2).

3.2 National legislation

3.2.1 Greece

3.2.1.1 The right to private life and the protection of personal data under the Greek Constitution

The right to private life

Under article 9(1) of the Greek Constitution, "the private and family life of an individual is inviolable". As a significant aspect of the free development of personality, the right to private life is expressly stipulated in the 1975 Constitution, influenced by the provisions of Article 8 of the 1951 European Convention on Human Rights on the right to respect of a person's private and family life, home and correspondence[250]. The right to private life constitutes a right with evolving concept and scope. In order to meet current protection safeguards, in light of technological advancements in the sector of information and communication, as well as of the intrusion of the mass media and the internet into a person's private sphere, an evolving interpretation is deemed necessary. In the context of article 9(1) of the Constitution, the individual is protected against intrusion from others, public authorities or other natural and legal persons.

The right holders are natural persons, nationals and non-nationals and under conditions persons under the 18 years of age. With regard to children (persons under the age of 18), their right to privacy is guaranteed under article 16 of the 1989 United Nations Convention on the Rights of the Child, which has been ratified by the law 2101/1992. This should be considered in conjunction with the Civil Code regulating legal capacity and legal custody of parents and legal guardianship.

Main infringements of the right to private life can be a) the disclosure of an individual's personal data related to his/her private sphere without his/her consent or with no legal and justified grounds in the public interest, b) the surveillance with the use of technology and devices, which can result in the disclosure of data containing sensitive information and place a risk to the individual's fundamental rights and freedoms, and c) transmission of information related to an individual's private life[251].

The right to private life is connected with articles 9 A of the Constitution on the right to the protection of personal data and article 19(1) on the right to communications confidentiality and thus must be examined in conjunction. All the aforementioned comprise the principal aspects of an individual's private sphere, especially with regard to communication and exchange and transmission of information and data.

The right to the protection of personal data

In article 9 A of the Greek Constitution it is stipulated that 'All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as

[250] See also Ακριβοπούλου Χ.Μ., Άρθρο 9, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017.

[251] Δαγτόγλου Π. *Δ.*, Συνταγματικό δίκαιο, Ατομικά δικαιώματα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2012, p. 331.

specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law'. This clause has been introduced with the 2001 revision of the Constitution in alignment with European standards. Within the scope of this provision falls every information which relates to an identified or identifiable natural person in the context of both his/her private sphere and in the public sphere[252,253]. In addition, it includes all aspects of intervention and not solely automated processing, though the risks of technological developments are considered. Limitation to the right can be imposed only where provided by law setting requirements such as the informed consent of the data subject or the exercise of other rights (e.g. to information, to freedom of expression, to a legal claim) or a public interest (e.g. the investigation of crimes)[254]. In any event, the principle of proportionality, as stipulated in article 25 of the Constitution, must be met and the respect and protection of the value of the human being should be guaranteed[255,256].

The right to personal data protection concerns every natural person. Legal persons' data are not personal data. Under the constitutional provision, state authorities, bodies and agencies shall ensure the unhindered implementation of the right and for this shall take also safeguard measures[257]. Furthermore, an independent authority must be in place to ensure the implementation of the right to personal data protection.

The right to confidentiality of correspondence

According to article 19(1) of the Constitution, 'secrecy of letters and all other forms of free correspondence or communication shall be absolutely inviolable. The guaranties under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes, shall be specified by law'. Though the article was stipulated in the 2001 Constitution's revision, within the meaning of correspondence, all current means of communication are included. This constitutional protection is provided for communications where the individual (a party) expresses a reasonable subjective expectation that the content and other elements of the communication will not be disclosed to third parties[258]. Data identified and protected in the course of communication comprise of the content of the messages transmitted, the data necessary for the establishment and maintenance of a communication (communication partners, time and duration of the communication; traffic data) and the data related to the location of the communication device employed (location data)[259]. Limitations to the right to confidentiality may be introduced in case (a) it is necessary for complying with a legal provision; (b) safeguards are in place

[252] See Council of State, Decision 1616/2012.

[253] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016, p. 10.

[254] Μήτρου Λ., Άρθρο 9 Α, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017, p. 225.

[255] Article 2(1) of the Constitution.

[256] See Council of State, Decision 3545/2002.

[257] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016.

[258] Παπαδόπουλος Ν., Άρθρο 19, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017, p. 477 citing ECHR case law.

[259] Παπαδόπουλος Ν., Άρθρο 19, in: Σύνταγμα, Κατ' άρθρο ερμηνεία, Φ. Σπυρόπουλος, Ξ. Κοντιάδης, Χ. Ανθόπουλος, Γ. Γεραπετρίτης (eds.), Εκδόσεις Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2017.

that prohibit any infringement of the constitutional statutes; (c) there is court order to do so; (d) this serves the purposes of public security and the investigation of serious crimes[260].

3.2.1.2 Legal framework on personal data protection and processing

3.2.1.2.1 Main provisions

The principal legal instrument regulating the protection of personal data is up until May 2018 law 2472/1997 as amended[261], which was originally adopted to transpose the 'Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data' into national law. However, from 25 May 2018 and on, the General Data Protection Regulation will come into force directly in all Members States. Therefore, law 2472/1997 will be repealed. For the necessary changes and adjustments in national legislation, a new legal act has been proclaimed. The developed draft bill includes regulatory measures for the correct implementation of the GDPR nationwide and the transposition of the Police Directive into national law. Therefore, the law provides in Greek and within the Greek context all principles, measures, safeguards, processes, rules, exceptions and rights which are included in the GDPR and the Police Directive. A more concrete provision on making certain personal data public where a crime is being investigated is also foreseen. In addition, the upcoming role of the independent supervisory authority is laid down. Nevertheless, the draft bill has not been adopted yet (April 2018) and for this reason it is not possible to proceed with further description. In any event, the clauses of the GDPR, as spelt out, will come into force as expected.

3.2.1.2.2 The role of the Authority for the Protection of Personal Data

The role of the national supervisory authority, "the Authority for the Protection of Personal Data"[262], has changed by the introduction of the GDPR. To this end, no particular prior permission from the competent independent authority is necessary for the processing of personal data. To the contrary, the Regulation has established a certain procedure and safeguard measures to be applied in order for every controller and processor to know beforehand how compliance directly with the GDPR can be achieved. At the same time, the national supervisory authorities may set forth more concrete rules for processing activities that involve various categories of personal data and monitor the implementation of the GDPR in the country by providing consultation, conducting investigation, receiving complaints and issuing decisions. In the context of an investigation the member of the national authority has the right to have full access to the processing operations except for public security cases or for serious crime investigation[263].

[260] Δαγτόγλου Π. Δ., Συνταγματικό δίκαιο, Ατομικά δικαιώματα, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, 2012, σελ. 361.
[261] Consolidated version of the law, available at: http://www.dpa.gr/pls/portal/url/ITEM/E3BC3C1B7FC83BA6E040A8C07D24022A
[262] Website of the Greek Authority for the Protection of Personal Data available at: http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL
[263] Draft available at: http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf

All members of the Greek Authority for the Protection of Personal Data are bound by a duty of confidentiality. In case of any personal data leak by a member of the authority, the perpetrator is charged with fine or even incarceration and violations are regarded as cause of disciplinary action too. The national independent authority, pursuant to the provisions under articles 57 & 58 of the GDPR should, inter alia, encourage the drawing up of codes of conduct[264] and provide an opinion and approve such codes of conduct[265]; encourage the establishment of data protection certification mechanisms and of data protection seals and marks[266] and approve the criteria of certification[267].

3.2.1.3 Legal framework on electronic communications privacy

3.2.1.3.1 Main provisions and the case of disclosing communication

The primary legal instrument regulating privacy issues in the electronic communications sector is the law 3471/2006 which transposed the E-privacy Directive (2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector) into national law. Within the scope of the law falls any type of communication through land and mobile telephony, as well as the internet (public communications services & networks). Further on, by law 3674/2008 more safeguard measures were introduced such as obligations of the communication service providers to draft security policies, to encrypt voice messages, to record any processing activity, to inform the user and the supervisory authority where a personal data breach has occurred[268]. As the 2002 e-privacy directive was significantly amended by the Directive 2009/136/EC, law 3471/2006 had to be amended accordingly. Therefore, with the law 4070/2012 under articles 168-173 modifications were introduced to law 3471/2006[269].

The meaning of personal data breach has been broadened pursuant to the provisions of the amended e-privacy Directive, as new forms of breach were discovered[270]; 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service. In accordance, the obligations of the service provider where a data breach has occurred were more explicitly laid down pursuant to article 4(3) of the E-privacy Directive[271].

With regard to the security of processing and without prejudice to the principal legal instrument on data protection (be it previously the Directive 95/46/EC and now the GDPR), the service providers must ensure that personal data can be accessed only by authorised personnel; protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and

[264] See article 40(1) GDPR.
[265] See article 40(5) GDPR.
[266] See article 42(1) GDPR.
[267] See article 42(5) GDPR.
[268] Available at: http://www.adae.gr/fileadmin/docs/nomoi/N.3674.2008.pdf
[269] Consolidated version of the law 3471/2006, available at: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/N3471_06.PDF
[270] Article 2(11) Law 3471/2006.
[271] Article 12(2) Law 3471/2006.

unauthorised or unlawful storage, processing, access or disclosure; and ensure the implementation of a security policy with respect to the processing of personal data[272].

Provisions on traffic data and location data, as previously analysed, cover not only the new forms of services provided through land and mobile telephony, but also the services provided by social networking sites[273]. Processing of location data is prohibited unless the user has provided his/her consent (which can withdraw at any time) or the competent authorities for emergency situations or law-enforcement and judicial authorities, first aid services and fire-brigade request the location data to identify the call and further to manage an emergency or investigating a crime[274].

Confidentiality of communications may be restricted only in compliance with the Constitution. Law 2225/1994 regulates the lifting of confidentiality according to the constitutional statute for the purposes of either public security or the investigation of serious crimes[275]. In the latter case, lifting of confidentiality can be ordered by the Judicial Council after a request from the Public Prosecutor or the Investigating Magistrate. Within 24 hours, the Council must issue a decision. In exceptional cases, the Public Prosecutor or the Investigating Magistrate can order the lifting of confidentiality and within 3 days, they have to introduce the request before the competent Judicial Council. Additional safeguard action has to be taken for the prevention of abusing such measures. Consequently, for each order for lifting confidentiality the Authority for Communication Security and Privacy, the competent Minister (of Justice) and to the body in charge (management committee/ council/ board) of the legal person of the communication service provider or network must be notified. Moreover, the competent judicial authority shall write a report for each order issued concerning the lifting of confidentiality; the measure has to be limited to the minimum necessary duration and the user (data subject) holds the right to be notified after the measure has been taken.

3.2.1.3.2 The role of the Authority for Communication Security and Privacy

The national independent authority for safeguarding the privacy of communications, the "Authority for Communication Security and Privacy"[276], was established with Law 3115/2003 (article 1)[277], pursuant to article 19(2) of the Greek Constitution. The authority is, inter alia, responsible for monitoring the cases were lifting of confidentiality has been employed; carries out investigations; receives complaints; keeps a record of personal data processing and provides advices on issues of

[272] Article 12(3), law 3471/2006.

[273] Μίτλεττον Φ., Η έννοια των προσωπικών δεδομένων, in: Προσωπικά δεδομένα, Κοτσαλής Λ. (ed.), Νομική Βιβλιοθήκη, 2016, Νομική Βιβλιοθήκη, 2016.

[274] Article 6(4) & (5) Law 3471/2006 as amended.

[275] Lifting of Confidentiality is permissible for the investigation of felonies under:

(a) articles 134, 135(1)&(2), 135 A, 137 A, 137 B, 138, 139, 140, 143, 144, 146, 148(2), 150, 151, 157(1), 168(1), 187(1)&(2), 207, 208(1), 264 points (b)&(c), 270, 272, 275 point (b), 291(1) point (b)&(c), 229, 322, 324(2)&(3), 374, 380, 385 of the Penal Code; Article 4(1) point (a) of law 2225/1994 as amended by Law 3658/2008. Kidnapping for the purpose of ransom or kidnapping of a child under 14 years old falls under this provision.

[276] Website of the Hellenic Authority for Communication Security and Privacy available at: http://www.adae.gr . Relevant legislation available at: http://www.adae.gr/nomothetiko-plaisio/elliniki-nomothesia/nomoi-gia-to-aporrito-epikoinonion/

[277] Available at: http://www.adae.gr/fileadmin/docs/nomoi/N.3115-2003.pdf

privacy. According to the amended article 6(4) of Law 3471/2006, the national authority issues acts where the procedure, the means any other technical detail for disclosing location data is described.

3.2.2 Belgium

3.2.2.1 The right to private life and the protection of personal data under the Belgian Constitution

The right to private life (and family life)

The Belgian Constitution provides the right to respect for private and family life in Article 22 and the right to freedom of expression in Articles 19 and 25**.** In addition, it regulates the right to respect of a person's home (*Article 15*) and the right to secrecy of communication (*Article 29*).

In addition, there are several specific laws in Belgium that include provisions protecting the right to privacy, such as:

- The Law on the protection of privacy in relation to the processing of personal data (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens|Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*) (DPL) of 8 December 1992.
- The Belgian Criminal Code provides criminal sanctions for certain infringements of private and family life, including:
    - telephone tapping (*Article 314bis*);
    - violation of domestic privacy (*Article 439*);
    - stalking and mobbing (*Article 442bis and ter*);
    - libel (*Article 443 to 447*);
    - professional secrecy (*Article 458*);
    - secrecy of correspondence (*Article 460 to 460ter*).

In addition, there are various laws and regulations containing privacy rights that relate to specific situations, including employee rights, patient rights, electronic communications, installation and use of surveillance cameras.

Belgium is also a signatory to several international conventions (including the European Convention on Human Rights) that provide protection of an individual's right to privacy and the right to freedom of expression.

The right to protection of personal data

The Data Protection Directive has been implemented into Belgian law by the Law on the protection of privacy in relation to the processing of personal data (*Wet tot bescherming van de persoonlijke*

levenssfeer ten opzichte van de verwerking van persoonsgegevens|Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) (DPL) of 8 December 1992 (as subsequently amended), which entered into force on 1 September 2001. The DPL has been further implemented by the Royal Decree of 13 February 2001 (*Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*).

Sectoral laws

Belgium has not adopted a genuinely "sectoral" approach for the regulation of the protection of privacy and personal data, but has nevertheless adopted specific rules for certain cases. In addition to the DPL and the Royal Decree of 13 February 2001, a number of specific laws and rules also contain provisions on the protection of privacy and personal data, such as:

- The installation and use of surveillance cameras (except for cases subject to specific regulations) is governed by the Camera Surveillance Law of 21 March 2007 (Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's/Loi réglant l'installation et l'utilisation de caméras de srveillance).

- The installation and use of surveillance cameras for monitoring employees is subject to Collective Bargaining Agreement No. 68 concerning the camera surveillance of employees of 16 June 1998 (*Collectieve arbeidsovereenkomst 68 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats/Convention collective de travail 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail*).

- Monitoring of employees' online communication is regulated by Collective Bargaining Agreement No. 81 concerning the monitoring of electronic communications of employees of 26 April 2002 (*Collectieve arbeidsovereenkomst 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische onlinecommunicatiegegevens/Convention collective de travail 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau*).

- The implementation of exit checks for employees with a view of preventing theft in the workplace is regulated by Collective Bargaining Agreement No. 89 concerning the prevention of theft and exit checks for employees leaving the company or the workplace of 30 January 2007 (*Collectieve arbeidsovereenkomst 89 bettrefendre de diefstalpreventie en de uitgangscontroles van werknemers bij het verlaten van de onderneming of de werkplaats/Convention collective de travail 89 concernant la prévention des vols et les contrôles de sortie des travailleurs quittant l'entreprise ou le lieu de travail*).

- The Electronic Communications Law of 13 June 2005 (*Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques*) contains provisions on the secrecy of electronic communications and the protection of privacy in relation to such

communications.

- The Patient Rights Law of 22 August 2002 (*Wet betreffende de rechten van de patient/Loi relative aux droits du patient*) regulates, among other things, the use of patients' data and the information that patients need to receive in respect of this use.

3.2.2.2 Legal framework on personal data protection and processing

3.2.2.2.1 Main provisions

In order to meet GDPR requirements, additional implementing legislation is expected. However, no drafts have been made public and the timeframe is uncertain.

3.2.2.2.2 The role of the Authority for the Protection of Personal Data

The General Data Protection Regulation (EU) 2016/679 creates a new privacy regime immediately applicable across the EU as from 25 May 2018. Under the GDPR, national supervisory authorities will have a strengthened role and increased enforcement powers.

In order to meet GDPR requirements, the Belgian legislator has adopted a law reforming the current Belgian Privacy Commission. The law was submitted in the Chamber of Representatives on 23 August 2017 and was approved by the Parliament in plenary meeting on 16 November 2017.

The main purpose of the new law is to reform the existing Privacy Commission (*"Commissie voor de Bescherming van de Persoonlijke Levenssfeer" – "Commission de la Protection de la Vie Privée"*) to ensure that it can fulfil its tasks in accordance with the GDPR as from 25 May 2018. Unlike the current Privacy Commission, which has limited prosecutorial and no direct sanctioning powers, the new "**Data Protection Authority**" is to become a real investigative and sanctioning authority.

The name of the new authority will be "*Gegevensbeschermingsautoriteit*" in Dutch and "*Autorité pour la protection des données*" in French.

Composition of the reformed Authority

The law provides for a structural change of the composition of the current Belgian Privacy Commission. The existing sector committees (responsible for controlling the lawfulness of sector-specific data processing activities) will be replaced by six new bodies:

- An **Executive Committee** (*"Directiecomité" – "Comité de Direction"*) responsible for defining the general policy of the Authority, including the use of the annual budget;
- A **General Secretariat** (*"Algemeen Secretariaat" – "Secrétariat general"*) taking care of the daily operations of the Authority (e.g. providing advice on Data Protection Impact Assessments, creation of an accreditation system for certification bodies, adoption of standard contractual clauses, etc.);
- A **Front-line Service** (*"Eerstelijnsdienst" – "Service de première ligne"*): the intermediary player between data subjects and the inspection and litigation bodies. This body receives requests and

complaints, starts mediation procedures, provides information and makes efforts to raise awareness;

- A **Knowledge Center** (*"Kenniscentrum" – "Centre de Connaissance"*) issuing advice and recommendations on GDPR compliance;
- An **Inspection Body** (*"Inspectiedienst" – "Service d'inspection"*): the investigating body of the Data Protection Authority having an extensive range of investigative powers; and
- A **Dispute Chamber** (*"Geschillenkamer" – "Chambre contentieuse"*): a legal and administrative body holding the prosecution and sanctioning powers. Appeals against the decisions of the Dispute Chamber will be dealt with by the Market Court (*"Marktenhof" – "Cour des Marchés"*) of the Brussels Court of Appeal.

These six bodies may be assisted by **experts** in the exercise of their tasks. The experts may come from different sectors (academic, private and public sector, civil society, etc.). Their advice will not be binding.

The Data Protection Authority will also regularly consult a **Reflection Council**, who reflects the society in its entirety and who will be providing non-binding advice to the Authority.

Powers of the reformed Authority

The powers of the Data Protection Authority may be summarised into four categories, in order of priority**:**

- **Providing information and advice** to individuals, controllers, processors and policy makers to enforce or comply with data protection legislation;
- **Assisting** controllers and processors to make maximum use of the prevention tools provided for in the GDPR, such as certification, adherence to codes of conduct, appointment of a Data Protection Officer (DPO), etc.;
- **Monitoring** of controllers and processors, and carrying out investigations, through the Inspection Body.
- **Imposing sanctions**, ranging from a simple warning to administrative fines amounting up to 20 million EUR or 4% of the total worldwide annual turnover of the infringing undertaking, whichever is higher.

3.2.2.3 Legal framework on electronic communications privacy

3.2.2.3.1 Main provisions and the case of disclosing communication

The basic law regulating telecommunications in Belgium is the federal Electronic Communications Act of 13 June 2005 (Electronic Communications Act), which replaces most but not all of the provisions of the federal law of 21 March 1991. The Electronic Communications Act covers all essential fields of

electronic communications, including:

- Defining the objectives and powers of the national telecommunications regulator, the Belgian Institute for Postal Services and Telecommunications (BIPT).
- Establishing specific regulations for telecommunication operators in relation to the notification requirements for the provision of electronic communications services and networks, the use of numbers and radio frequencies, shared use of sites and infrastructure, administrative fees, terminal equipment, directories and enquiry services and cryptography.
- Protecting fair market competition (for example, market analysis and the determination of significant market power (dominance), the imposition of regulatory obligations and so on).
- Protecting public interest, society and consumers (for example, universal service obligations, services of public interest and the protection of final users (including information of end users, quality and security of services, the provision of supplementary services, secrecy of communications, and the processing of personal data)).

The Electronic Communications Act was amended in 2012, 2014 and 2017, notably to implement the amended EU regulatory framework for telecommunications. A great number of Royal Decrees implement the various aspects covered by this Act.

The two other relevant federal Acts are the:

- Act of 17 January 2003 regarding the statute of the regulator BIPT.
- Act of 17 January 2003 on the appeals and dispute settlement arising from the law of 17 January 2003 on the statute of the regulator of the Belgian postal and telecommunications sectors.

Both acts have also been amended a few times, the last one by the federal law of 16 March 2015 to further ensure the independence of the BIPT following the intervention of the European Commission.

The Law of 8 December 1992 on the protection of privacy with respect to the processing of personal data applies to the telecommunications sector. This was amended by the Law of 11 December 1998, which implemented Directive 95/46/EC on data protection (Data Protection Directive) into Belgian law. The Law of 1992 was subsequently amended by the Law of 21 February 2003.

The 1995 EU Directive has been revised through the adoption in April 2016 of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)). The EU additionally adopted Directive 2016/21148/EU concerning measures for a high common level of security of network and information systems in July 2016, regulating cybersecurity standards for essential infrastructure at EU level for the first time. Both measures will take effect in May 2018. A separate directive adopted at the same time as the GDPR governs the data protection and data breach notification of public authorities processing personal data in the context of criminal law.

The GDPR grants regulatory authorities stronger investigative and enforcement powers and the ability to impose high fines for infringements of the legal framework regarding data protection. The exiting Belgian Commission for the Protection of Privacy was not authorised to impose fines and had to refer cases to the public prosecutor's office. Under the Law of 3 December 2017, the Belgian Data Protection Authority will have increased investigative and enforcement powers, such as the power to conduct on-site reviews and to impose administrative fines. The GDPR also requires all companies that process personal data to implement appropriate technical and organisational measures, such as pseudonymisation and encryption, to ensure a level of security that is appropriate to the risk.

Before the adoption of the GDPR, the Commission for the Protection of Privacy issued in December 2016 recommendations on the right to data portability, identification of the lead authority and the requirement to appoint a data protection officer. These recommendations were updated in May 2017.

The current Belgian general data protection rules contain numerous requirements regarding the processing of personal data. The Electronic Communications Act also creates a specific regime for operators (providers of electronic communications services) (based on the e-privacy directive also under revision by the EU institutions) in relation to the:

- Processing of data.
- Secrecy of communications.
- Protection of privacy.

Firstly, under the Electronic Communications Act operators must destroy all data traffic from subscribers or final users, or make such data anonymous, as soon as the information is no longer necessary for the transmission of the communication (*Article 122, section 1, Electronic Communications Act*) (although this is subject to the obligation to co-operate with the judicial authorities). However, an exception to this general rule applies in relation to limited data for the purposes of billing, marketing and investigating fraud (*Article 122, sections 2 to 4, Electronic Communications Act*). In this context, data can only be processed by the person responsible for billing, traffic management, the processing of client inquiries, fraud detection, marketing, and (under certain conditions relating to the end-user's consent) the provision of services with traffic and location data (*Article 122, section 5, Electronic Communications Act*). The processing of data must also be strictly limited to what is necessary for the exercise of these activities.

Secondly, the Electronic Communications Act protects the secrecy of communications (*Article 124*, *Electronic Communications Act*). This includes clear prohibitions on intentionally doing the following:

- Gain knowledge of the existence of information transmitted through electronic communications.
- Identify persons concerned by the transmission of information and its contents.
- Gain knowledge of electronic communications data regarding another person.
- Process or use any information, identification or data obtained.

A number of very limited exceptions to the principle of secrecy of communications are provided for in Article 125. Operators must notably co-operate with judicial authorities and therefore retain traffic data and make them available to the authorities.

In January 2017, the European Commission published a draft e-Privacy Regulation that would replace the current e-Privacy Directive. The new Regulation will also apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype and will ensure that these new services guarantee the same level of confidentiality as traditional telecoms operators. In September 2017, the Council of the European Union (the Council) proposed several amendments to the text.

Articles 126 and 126/1 of the Electronic Communications Act, which impose data retention obligation on operators, were modified in May 2016 following a judgment of the European Court of Justice (ECJ) of 8 April 2014.

In this judgment, the ECJ held that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) was invalid.

The ECJ stated that by requiring the retention of data by providers of public electronic communications services or networks, and by allowing the competent national authorities to access those data, the Data Retention Directive constituted an interference with the fundamental rights guaranteed by Article 7 (right to privacy) and Article 8 (protection of personal data) of the EU Charter of Fundamental Rights. The ECJ held that the Data Retention Directive did not provide clear and precise rules circumscribing the interference with these rights to what was strictly necessary. The data retention obligation generally covered all persons and all means of electronic communications and traffic data without any differentiation, limitation or exception. Furthermore, no objective criterion determined the limits of the access of the competent national authorities to the data and their subsequent use. Regarding the period of detention, no distinction was being made between categories of data.

On 11 June 2015, the Belgian Constitutional Court consequently annulled former Article 126 of the Electronic Communications Act containing the data retention obligation for operators, on the same grounds as those identified by the Court of Justice.

Under the newly modified Article 126 introduced by a law from May 2016, operators must retain the following categories of data:

- User and subscriber identification data (holder of the number/address).
- Connection and location data (place and duration of communication).
- Personal communication data excluding the content (origin and destination of the communication).

The competent authorities allowed to receive the data from the operators are the judicial investigative authorities, the intelligence and security services, the public prosecutor’s office, the emergency

services and the Ombudsman for Telecommunications. These authorities can only access specifically defined data for the purpose of executing specific tasks entrusted to them (for example, investigation of certain types of criminal offences, the search for missing persons or the localisation of persons in need of help).

Regardless of the category of data, operators must, as before, retain the data during 12 months.

In December 2016, the ECJ stated in a preliminary ruling that EU member states may not impose a general and indiscriminate obligation to retain data on providers of electronic communications services. Data retention must thus be targeted for the purpose of fighting serious crime. Additionally, the ECJ held that the national authorities' access to the retained data must be subject to conditions (including prior review by an independent authority). The ECJ held that any national legislation on the retention of data must:

- Be clear and precise.
- Provide for sufficient guarantees on the protection of data against risks of misuse, including by laying down the substantive and procedural conditions governing the access of the competent national authorities to the retained data.

In March 2017, the ECJ held in case C-536/15 opposing the Belgian company European Directory Assistance to Dutch operators Tele2, Ziggo and Vodafone-Libertal that under the Universal Service Directive the consent given by a telephone subscriber in any member states regarding the publication of its data in a public directory does not need to be renewed for the passing of the same data to an undertaking in another member states, if it is guaranteed that the data in question will not be used for purposes other than those for which the data were collected with a view to their first publication. The ECJ further held that such passing of data to another undertaking is not capable of substantively impairing the right to protection of personal data, as recognised by the EU Charter of Fundamental Rights.

In an opinion published in September 2017, the Belgian Institute for Postal Services and Telecommunications (BIPT) drew the consequences of this preliminary ruling and held that phone service providers must freely provide data to publishers of public directories, irrespective of their place of establishment.

Regarding cybersecurity, in 2014 the Centre for Cybersecurity Belgium (CCB) was set up by Royal Decree. The NISD promotes active co-operation among cybersecurity agencies at EU level.

In the electronic communication sector, the BIPT Council adopted on 14 December 2017 a decision regarding the thresholds and terms and conditions for reporting of security incidents within the electronic communications sector. This decision replaces the BIPT Council Decision of 1 April 2014 laying down the circumstances in which the operators must notify BIPT of a security incident and the terms and conditions of this notification. This decision specifies which security incidents have to be reported as well as the practical manner in which to report them.

Under the Belgian Code on Criminal Procedure, the public prosecutor is entitled to request operators of electronic communications networks to co-operate with them in relation to:

- Providing information enabling the identification of the subscriber and the electronic service subscribed to (*Article 46bis, Code on Criminal Procedure*).
- Demanding information from an operator regarding calls to and from a certain device (but not regarding the content of the call) (*Article 88bis, Code on Criminal Procedure*).
- Tapping telephone conversations (*Article 90ter to 90 decies, Code on Criminal Procedure*).

Electronic telecommunications providers must make accessible to judicial authorities, upon their simple request and without delay, data for the instruction and investigation for judiciary, security and intelligence purposes (*Article 126, section 2, Electronic Communications Act*). The new Article 126 of the Electronic Communications Act adds the emergency services and Ombudsman for Telecommunications to the list of competent authorities that are entitled to request access to newly defined categories of communications data. The data that can be requested from operators includes:

- Traffic data.
- Location data.
- End-user identification data.
- Service and terminal equipment data.

This duty of co-operation is implemented by Royal Decrees of 9 January 2003, of 12 October 2010 and of 19 September 2013.

For example, each operator must set up a "co-ordination unit" to which the competent authorities can address their requests. If the data is less than 30 days old, the data must be communicated in real time. If the data is more than 30 days old, the data must be communicated the next working day. Under new Article 126(1) of the Electronic Communications Act, not only judicial authorities but also emergency services and the Ombudsman for telecommunications are under certain conditions entitled to access communications data.

3.2.2.3.2 The role of the Authority for Communication Security and Privacy

There is no requirement under the DPL to notify personal data security breaches to data subjects or to the Privacy Commission.

However, Article 114/1, §2 of the Electronic Communications Law of 13 June 2005, as well as Commission Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches, require companies in the telecommunication sector to immediately (within 24 hours), notify personal data breaches to the Privacy Commission, who must transmit a copy of the notification to the Belgian Institute for postal services and telecommunications, Het Belgisch Instituut voor postdiensten en telecommunciatie/Institut belge des services postaux et des telecommunications (BIPT). If there is a breach of personal data or privacy of individuals, the company must also notify the data subjects affected by the breach.

A telecommunications company is exempt from the obligation to notify personal data breaches to the data subject if:

- The company asks the Privacy Commission for permission to postpone the notification to the data subject if the notification may endanger the investigation of the breach of personal data.
- The company can show that it has applied sufficient technical protection measures to protect the personal data that was subject to a breach. Such measures shall render the data unintelligible to any person who is not authorised to access it.

In order to facilitate the notification of personal data breaches, the Privacy Commission has published an electronic notification form specifically addressed to telecommunications operators.

Although notification of personal data breaches is not legally required in sectors other than the telecommunications sector, the Privacy Commission published a Q&A on data breaches on its website. In this Q&A, the Privacy Commission encourages all data controllers to notify data breaches, (including data controllers outside the telecommunications sector). The Privacy Commission also published on its website a general notification form that can be used by companies from sectors other than the telecommunications sector.

BIPT is a federal institution which performs several tasks. As the regulator of the electronic communications market is, inter alia, has the task of promoting completion, contributing to the development of the internal market and protecting the users'interests.

4 General Ethical Aspects related to regulations and technical aspects of mobile applications

4.1 Compliance with the current national, EU and International legislation

As it is already mentioned above (Section 3.1 European legislation), missing children investigation and rescue involves, among others, the storage and processing of personal data of the missing child and his/her family's members. In the context of ChildRescue Platform other individuals are also involved, mainly as data sources and data administrators during the investigation process, including several types of users, actors and authorities. In this context, legislation concerning data protection and personal data processing shall be taken into consideration, in order to ensure the compliance of the ChildRescue Platform with current international, European and national legal provisions.

4.1.1 Agreements, laws and regulations (including EU directive on data protection)

At a national level, ChildRescue should be in alignment with the national legislation concerning personal data administration, as is presented in the respective section of the Chapter 3.2. Moreover, EU and international legislation should be taken into account in order to avoid any data misuse.

4.1.1.1 Pre-define the legislation to be followed in cases than more than one countries involved in a case

A number of cases of missing children are related to international kidnappings, unaccompanied refugee and immigrant children, forced disappearances and so on. In such cases, where movement of a child in more than one countries takes place, it should be pre-decided which legislation prevails concerning personal data of involved parties in the context of the ChildRescue Platform. It should be, namely, pre-decided whether the legislation of the country where the child declared as missing will apply or the legislation of the country where the child has been seen and/or found or the EU or international data protection relevant legislation.

4.1.1.2 Pre-define the level of access of authorities requesting data-personal identifiers of 'community sensors'

'Community sensors', namely sources of information who are also subjects of data can be *registered identifiable users*, *registered users without personal identifiers* and *anonymous users*. Considering the two last groups, *registered users without personal identifiers* and *anonymous users,* they hypothetically are able to provide information for a case of a missing child *anonymously.* Authorities, however, like Prosecutor or the Police, may ask the Platform operator (or the data processor) to identify such a non-validated or non-registered user. The level of access in personal data of these groups of users should be clearly pre-defined in order to avoid any type of privacy violation and at the same time the Platform to operate according to the law.

**Despite users are not registered, some basic information may collected and stored automatically in the server where ChildRescue Platform is hosted, when users are using the platform and/or the*

mobile application (such as the name of the internet domain if they are using a private internet access account, the Internet Protocol (IP) address, the date, time and place they used the mobile app).

4.2 Acquiring National Data Protection Authorities' licenses

ChildRescue operating organisations shall submit request to the National Data Protection Authority in order to obtain license for establishment and operation of register containing sensitive personal data. In this license should be clearly and detailed defined the following: type of license; purpose of the registry maintenance; identity of data processor; type of data; sources of data; duration of license; terms and conditions for granting the license according to the currently applied legislation.

In case the operating organisations are already granted with a similar license, they should inform respectively the National Data Protection Authority for the additional usage (ChildRescue Platform and App) and to proceed with the modification, if necessary.

4.2.1 Including secondary use of data

In the detailed description of the purpose of the registry and of data processing, particular reference should be made to the secondary use of data. Such secondary use can be, for example, sensitization of the community and activation of its sources towards supporting families in crisis and in particular towards the prevention of child disappearances and the more efficient management of cases of children declared as missing.

4.3 Obtaining parental/guardian informed consent before using child's data

Similarly to other systems/programs of communicating information of missing children (such as the Amber Alert) parental/legal guardian informed consent should be obtained before using child's personal data in the context of ChildRescue Platform and application, along with the permission of the Police (or other responsible authority). A standardized informed consent form is recommended to be developed on the basis of which missing child's parent/legal guardian will allow the use (upload and dissemination) of child's personal data through ChildRescue Platform and application.

4.3.1 Including secondary use of data

It should be decided whether obtaining of parental/legal guardian consent for secondary use of child's personal data will be part of the consent for using child's data for the investigation process via ChildRescue platform or will be a quite different process and document.

The decision should be made after considering the strengths and limitations of obtaining one or two different parental consent for main and secondary use of personal data respectively.

Note: *"Secondary use of the data is required for the validation of the platform and methodology, the performance of statistical analysis, academic research and dissemination of the project's results.*

Publication of the results of these analyses will not include any personal case-specific information and will only appear in the form abstractions or aggregates".

4.4 Acquiring agreements with third parties

In order to promote community participation during investigations for missing children, the ChildRescue Platform may use third-party websites (including social media platforms such as Facebook, Twitter, and Instagram). Agreements should be acquired with third parties containing terms and conditions of cooperation (it should be clear, for example, that third party service provider's terms of service and privacy policies govern ChildRescue users activity on the third party website or whether ChildRescue Platform intents to collect and maintain personal data the users make available on third party websites).

In addition, appropriate agreements may be considered with providers of telephone services, given the nature of ChildRescue mobile application.

4.5 Mobile Application-related Ethical aspects

Privacy by design is a technical approach to a social problem.[278] Concerning limits of privacy by design, Danezis *et al.* (2014)[279] noted that there is a caveat: a significant part of the low-level privacy invasion is the direct result of the internal functioning of technical systems. Thus, while the incentives and will to invade privacy may be social problems, the actual ability to do so is a technical problem in many instances. Thus, dealing with it at the technology level is necessary. The same concerns can be considered for mobile applications too.

4.5.1 Applying privacy design principles-ensuring appropriate level of sensitive personal data protection

The above mentioned (in Chapter 3) Directive 2002/58/EC (*ePrivacy Directive*) can be interpreted as call for privacy by design while EU data protection law, Art. 29 Data Protection Working Party ask for and refer to privacy by design; there, practical aspects are also highlighted: "In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives. In particular, when making decisions about the design of a processing system, its acquisition and the running of such a system the following general aspects / objectives should be

[278] Gürses, J. S. (2014). Can you engineer privacy? Communications of the ACM, 57(8):20–23

[279] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, JH., Le Métayer, D., Tirtea, R., Schiffne, S. (2014). Privacy and Data Protection by Design–from policy to engineering. European Union Agency for Network and Information Security-ENISA Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

respected: Data Minimization; Controllability; Transparency; User Friendly Systems; Data Confidentiality; Data Quality; and Use Limitation".[280]

Mobile apps often rely on user data-including contact information, location, photos, and so on-all of which can be vulnerable to data breaches. Before releasing ChildRescue application it should be ensured that security policies are set appropriately and that the right measures to protect the data that users ("community sensors") share with the app. Some indicative tips for developers towards mobile app security include, among others, review of data to collect and maintain and creation of secure users' credentials (usernames and passwords).[281]

4.5.2 Ensuring prevention of application misuse (by any potential stakeholder of the application)

The challenge for developers of a mobile app is anticipating misuse and designing to prevent it. Providing that ChildRescue is dealing with children's data, it should be ensured that necessary standards and regulations are applied in order to prevent any misuse of application. Ways to prevent data misuse via the platform and application should be explored (such as monitoring of data access; monitoring of various stakeholders/users actions; and ensuring that the system is well-protected, as data misuse is considered a security breach and first and foremost it is a security concern[282]).

4.5.3 Transparent administration of log files (content; protection; access; destruction)

The first ethical dilemma mentioned in a popular article in InfoWorld[283] is about log files, what to save and how to handle them. It is noted that developers often keep records of everything, because this is the only way to debug a system. Log files, however, can expose information that users want kept secret. The mere existence of log files begs several ethical questions. Are they adequately protected? Who has access? When we say we destroy the files, are they truly destroyed? The crucial point, valid also for the ChildRescue Platform, is to decide what information is worth keeping, given the ethical risks of doing so.

4.5.4 Pre-define aspects of platform maintenance

Monitoring process and methodology for ensuring the smooth operation of platform and application should be defined as well as the responsible organisation/authority to undertake the monitoring and consequently the reporting to data processor.

---

[280] Ibid.

[281] Source: https://www.sba.gov/blogs/developing-mobile-app-follow-these-12-tips-protecting-and-securing-user-data

[282] Source: https://www.ekransystem.com/en/blog/4-ways-detect-and-prevent-misuse-data

[283] Source: https://www.infoworld.com/article/2607452/application-development/12-ethical-dilemmas-gnawing-at-developers-today.html

5 Ethical Provisions related to non-technical aspects of individual Functional Components

5.1 Collaboration space

The first component of the ChildRescue Platform is a *collaboration space* allowing all investigators to securely share location-based multi-media information regarding the investigation in groups, with specific access rights, or publicly. Real-time messaging will be granted among the voluntary organisation and rescue team members, as well as with citizens who have provided evidence for the missing person. In this space, all contributors to the investigation will be also able to provide their perspective about the missing person through a collective tagging dashboard.

Given the importance of *collaboration space* component it is important to take into account ethics related to non-technical aspects during the development of the platform such as the following.

5.1.1 Ensuring user friendly interface

Real time messaging, collaborative tagging and data sharing are all actions that various users will be called to undertake –often in restricted time- when they will use the ChildRescue Platform and app. In order to facilitate the right usage of the app by the users or, otherwise, to minimise the risk of misuse by mistake, a user friendly interface should be ensured. There are numerous studies and examples on how to design a "perfect mobile app user interface" including suggestions about colours, fonts, icons (App Icons – for representing an app; Clarifying Icons – explain certain tasks; Interactive Icons – used mainly for navigation; Decorative Icons – created for a more attractive look;) and navigation tools; moreover, guidelines are available for developers (related, for example, to consistency and simplicity of the interface -not to create the sensation that customers need instruction manual for using the app; to use only needed and essential information without overloading the app; to avoid ambiguity-everything should be as clear as possible, without the possibility of misinterpretations; and so on).[284]

Additionally, through an easy-to-use interface, app users provided with the ability to set their privacy settings, namely they have direct control over their own personal data. As for the user friendly systems it is noted that "*privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users*".[285]

[284] Source: https://appsamurai.com/6-necessary-elements-for-designing-a-perfect-mobile-app-user-interface/

[285] Source: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport

5.1.2 **Terms of Use for main investigators** (national authorities, volunteer organisations and rescue teams)

In order to ensure appropriate use of the ChildRescue platform and app during cases' investigation process and at the same time to prevent misuse of the system or breath of confidentiality and data privacy, detailed "Terms of Use" is recommended to be drafted –although it is not mandatory by law- concerning all groups of main investigators (national authorities, volunteer organisations and rescue teams) and taking into account their specific roles and level of access in the platform. Various templates are available online that may be used as a basis for preparing such a document for the needs of the specific platform and app (sample)

5.1.3 **Code of Ethics of professionals provide and administrate information**

Main professional specialties to be involved in the ChildRescue Platform either as sources of data or as data administrators are already subjected in (national and international) professional codes of ethics [Psychologists (Ethical Principles of Psychologists and Code of Conduct); Social Workers (Code of Ethics-NASW); Sociologists (Code of Ethics-International Sociological Association)]; to this end, they shall considered as *eligible* in terms of ethics for the ChildRescue.

5.1.4 **Detailing step-by-step instructions for data sharing, real-time messaging and collaborative tagging**

Detailing step-by-step instructions for data sharing, real-time messaging and collaborative tagging should be included in both, Terms of Use for main investigators (national authorities, volunteer organisations and rescue teams) and Terms of Use for users-*community sensors,* as all of them are expected to be involved in these activities in platform's collaborative space.

5.1.5 **Privacy Policy**

The EU legal framework (Data Protection Directive (95/46/EC) applies in any case where the use of apps on smart devices involves processing personal data of individuals**.** The ePrivacy directive (2002/58/EC, as revised by 2009/136/EC) sets a specific standard for all parties worldwide that wish to store or access information stored in the devices of users in the European Economic Area.

ChildRescue is expected to collect, store, and share personal data (e.g. names, email addresses, IP addresses, location data etc.) of missing children as well as of other groups of users and, therefore, a privacy policy is mandatory, as both the above directives are imperative laws in that the individual's rights are non-transferable and not subject to contractual waiver.

Therefore, an easily accessible privacy policy shall be drafted to inform users at least about

- what is ChildRescue (identity and contact details)
- what personal data the app collect and process and why this is necessary (purpose)
- whether personal data will be disclosed to third parties (if yes, specifically to whom)

- what are their (users') rights, in terms of withdrawal of consent and deletion of data

Content of the privacy policy could be structured as follows:

- Information Collected by the app

- Information Shared with Third Parties

- Cookies

- Security

- Information from Children Under the Age of 13

- Questions

Note: Concerning Privacy Policy changes in project's GA is mentioned that *although most changes are likely to be minor, ChildRescue may change its Privacy Policy from time to time, and in ChildRescue's sole discretion, after acceptance by the consortium, the EAB and the responsible national agencies. ChildRescue will inform users for any such change, asking for their acceptance, in order to continue using of the platform. User's that have not accepted the revised policies will be put into a "frozen" state, meaning that their data will not be shared anymore until they decide to accept or reject the new policies. Rejecting them, would mean that user's data will be treated using the previous policy, while users will also be able to choose to delete their account and remove their data from the platform.*

5.1.6 Terms of Use of mobile app for community users-sources of information /'community sensors'

Similarly, as for the groups of main investigators (national authorities, volunteer organisations and rescue teams), a detailed "Terms of Use" is recommended to be drafted –although it is not mandatory by law- concerning all groups of community users (registered identifiable users; registered users without personal identifiers; and anonymous users).

5.1.7 Safeguarding users' privacy and confidentiality of personal data

ChildRescue should follow necessary procedures to ensure that all staff and others who have access to any personal information held by the Platform and App, are fully aware of and abide by their duties and responsibilities under the main EU legal framework.[286] Duties and responsibilities could be described either as part of the Terms of Use of main investigators' groups or in a separate "Data Protection and Confidentiality Policy" document which will be developed.

[286] namely Data Protection Directive 95/46/EC; The ePrivacy directive 2002/58/EC as revised by 2009/136/EC

5.1.7.1 Inform users about what personal information the app may access, collect and use, how and why the information will be used and how they can control this use

This information should be clearly provided to users in the context of Privacy Policy; in addition, they should be informed on whether and how they can control the use of their personal data, providing them with appropriate tools (see above "Ensuring user friendly interface" where it was mentioned that "*…through an easy-to-use interface, app users provided with the ability to set their privacy settings, namely they have direct control over their own personal data*".

5.1.8 Notification engine

5.1.8.1 Ensuring user friendly presentation of information

5.1.8.2 Detailing step-by-step instructions for notifications' sharing

This chapter will be edited later when all related information is available. At this early stage it cannot be edited.

5.1.9 Data anonymisation & synchronization engine

5.1.9.1 Ensuring stakeholders' data privacy protection and anonymity at application and context layer (Data Privacy Management component)

5.1.9.1.1 Detailing anonymization method to be applied for children's data for secondary use

5.1.9.2 Pre-define aspects of platform maintenance (secure physical location of servers and graded access by different stakeholders)

5.1.9.2.1 Detailing method to by applied for case data archiving

This chapter will be edited later when all related information is available. At this early stage it cannot be edited.

5.1.10 Profiling engine

5.1.10.1 Selecting the appropriate variables

5.1.10.2 Ensuring confidentiality of sensitive personal data

5.1.10.2.1 Ensuring appropriate secondary data collection (from social networks, parents/guardians, professionals such as psychologists and social workers from the voluntary organisations)

5.1.10.2.1.1 Description of methodology for profiling and combined profile generation and tag management

This chapter will be edited later when all related information is available. At this early stage it cannot be edited. It will be completed as soon as the technical partners can provide details on the methodology.

5.1.11 Prediction engine

5.1.11.1 Selecting the appropriate method of analysis

5.1.11.1.1 Description of methodology to be applied for patterns matching (comparing archived cases with open cases); extracting of places of interest while protecting sensitive personal data and calculating the routes

This chapter will be edited later when all related information is available. At this early stage it cannot be edited. It will be completed as soon as the technical partners can provide details on the methodology.

5.1.12 Analytics engine

5.1.12.1 Ensuring data accuracy and completeness

5.1.12.1.1 Detailing methodology for validation and quality assurance of data

5.1.12.1.2 Detailing methodology for tracking investigation progress in real time

This chapter will be edited later when all related information is available. At this early stage it cannot be edited. It will be completed as soon as the technical partners can provide details on the methodology.

5.1.13 Data harmonization & interoperability space

This chapter will be edited later when all related information is available. At this early stage it cannot be edited. It will be completed as soon as the technical partners can provide details on the methodology.

6 Ethical issues related to unaccompanied minors

The term "unaccompanied migrant children" or "unaccompanied minors" describes all foreign national or stateless persons below the age of 18, who either arrive in the EU unaccompanied by a responsible adult or are left unaccompanied after their arrival. Most of them come from countries at war and/or poor living conditions so their ordeal pre-exists their terrifying journey.

The most common problems that migrant children face, are considered to be the following:

- Psychosocial challenges
- Lack of basic livelihood
- Sub-standard living conditions
- Separation from family
- Lack of adequate information
- Increased tension and stress
- Protection issues

These problems may be a huge burden upon any adult migrant, but they certainly exceed the response capabilities of an unaccompanied minor, regardless of specific age or gender. Furthermore, a child is particularly vulnerable to smugglers or traffickers, as well as to sexual violence and/or exploitation.

Unaccompanied children on the move are solely concerned about their survival and by the time they reach their destination, they are entirely depleted. Many of them, having suffered traumatic experiences on the way, have long – term effects such as depression, anxiety and post - traumatic stress disorder. Especially those that become separated from their parents along the migration route represent a challenge for professionals willing to support them. Nevertheless, they have to face a new series of problems upon arrival.

The United Nations Convention on the Rights of the Child (UNCRC) emphasizes that in all actions concerning children, whether undertaken by public or private bodies "the best interests of the child shall be a primary consideration". The UNCRC has been ratified by all EU Member States and its provisions are supposedly enshrined in all the relevant EU legislation and policies. Still, statistical data and real - life experiences prove that there remains a huge gap between theory and practice.

As soon as they arrive, children need to be identified as unaccompanied minors in order to receive protection; however this is not always possible since many of them do not have official documents, either because they were lost during the journey or they have never been issued at all. In such cases, EU Member States resort to various age assessing methods. The lack of consistency among age assessment practices across EU means that often children's accounts of their age may be questioned and examined repeatedly whenever they cross an internal border

6.1 Child Protection

6.1.1 Non- discrimination

The principle that distinctions should not be made between people or communities on any grounds of status, including age, gender, race, colour, ethnicity, national or social origin, sexual orientation, HIV status, language, religion, disability, health status, political or other opinion. This is connected to the fundamental principle of impartiality.

6.1.2 The best interests of the child (BIC)

The BIC encompass a child's physical and emotional safety (their well-being) as well as their right to positive development. In line with Article 3 of the United Nations Convention on the Rights of the Child (UNCRC), the best interests of the child should provide the basis for all decisions and actions taken, and for the way in which service providers interact with children and their families. Caseworkers and their supervisors must constantly evaluate the risks and resources of the child and his environment as well as positive and negative consequences of actions and discuss these with the child and their caregivers when taking decisions. The least harmful course of action is the preferred one. The Best Interests Principle must guide all decisions made during the case management process. Often in child protection there is no one ''ideal" solution possible, but rather a series of more or less acceptable choices that must be balanced with a child's best interests.

6.1.3 Seek informed consent

Informed consent is the voluntary agreement of an individual who has the capacity to give consent, and who exercises free and informed choice. In all circumstances, consent should be sought from children and their families or caregivers prior to providing services. To ensure informed consent, caseworkers must ensure that children fully understand: the services and options available (i.e. the case management process), potential risks and benefits to receiving services, information that will be collected and how it will be used, and confidentiality and its limits. Caseworkers are responsible for communicating in a child-friendly manner and should encourage the child and their family to ask questions that will help them to make a decision regarding their own situation.

6.1.4 Seek informed assent

Informed assent is the expressed willingness to participate in services. It requires the same child-friendly communication of information outlined above. However, for younger children who are by nature or law too young to give informed consent, but old enough to understand and agree to participate in services, the child's "informed assent" is sought.

6.1.5 Respect confidentiality

Confidentiality is linked to sharing information on a need-to-know basis. The term "need to-know" describes the limiting of information that is considered sensitive, and sharing it only with those individuals and sharing it only with those individuals who require the information in order to protect the child. Any sensitive and identifying information collected on children should only be shared on a

need-to-know basis with as few individuals as possible. Respecting confidentiality requires service providers to protect information gathered about the children and to ensure it is accessible only with a child's consent. Workers should not reveal children's names or any identifying information to anyone not directly involved in the care of the child. This means taking special care in securing case files and documents and avoiding informal conversations with colleagues who may be naturally curious and interested in the work. Importantly, confidentiality is limited when caseworkers identify safety concerns and need to reach out to other service providers for assistance (e.g. health care workers), or where they are required by law to report crimes. These limits must be explained to the children during the informed consent or assent processes. Supervisors and caseworkers should work together closely to take decisions in such cases where confidentiality needs to be broken.

6.2 Child Data Protection

Children are a particularly vulnerable category of Data Subjects, and the best interests of the child are paramount in all decisions affecting them. While the views and opinions of children should be respected at all times, **particular care should be taken to establish whether the child fully understands the risks and benefits involved in a Processing operation and to exercise his/her right to object and to provide valid Consent where applicable.**

Assessment of the vulnerability of children will depend on the child's age and maturity.

The Consent of the child's parent or legal guardian may be necessary if the child does not have the legal capacity to Consent. The following factors should be taken into account:

- Provision of full information to the parent or legal guardian and signature of the parent or guardian to indicate their Consent; and
- Ensuring the Data Subject is clearly informed and his/her views are taken into account.

The practice, not unknown in the humanitarian world, to ask for the impression of a fingerprint solely to confirm Consent is highly problematic since it can amount to the collection of biometric data and should therefore **be avoided**.

When using Consent, it is important to record any limitations/conditions for its use, and the specific purpose for which Consent is obtained. Where Consent has not been recorded, or no record of Consent can be found, the data should not be processed further (including transferred to a Third Party if there is no record of Consent for these purposes), unless it is possible to do so under a legal basis other than Consent (e.g. vital interest, legitimate interest or public interest).

Data Subjects have the right to object to the Processing and withdraw any Consent previously given at any stage of data Processing. In cases in which a Humanitarian Organisation suspects that Consent is being withdrawn under pressure from Third Parties, it is likely that the Humanitarian Organisation may be in a position to continue processing the Personal Data of the Data Subject on the basis of vital interests being at stake.

When Consent cannot be validly obtained, Personal Data may still be processed if the Humanitarian Organisation establishes that this is in the vital interest of the Data Subject or of another person, i.e. where data Processing is necessary in order to protect an interest which is essential for the Data Subject's life, integrity, health, dignity, or security or that of another person.

The Processing, including disclosure, of information is the most appropriate response to an imminent threat against the physical and mental integrity of the Data Subjects or other persons; or the processing is necessary to provide for the essential needs of an individual or a community during, or in the aftermath of, a Humanitarian Emergency.

In these cases, however, the Humanitarian Organisation should, if possible, ensure that the Data Subjects are aware of the Processing as soon as possible, that they have sufficient knowledge to understand and appreciate the specified purpose(s) for which Personal Data are collected and processed, and are in a position to object to the Processing if they so wish. This can be achieved preferably through direct explanations at the moment of the collection and, for example, during the provision of assistance.

EXAMPLE: A Humanitarian Organisation needs to collect Personal Data from vulnerable individuals following a natural disaster in order to provide vital assistance (e.g. food, water, medical assistance, etc.). It may use the vital interests of the individuals as the legal basis for the collection of Personal Data, without the need to obtain their Consent. However, it should 1) ensure that this legal basis is used only to provide such assistance; 2) offer the individuals the right to object; and 3) process the data collected in accordance with its privacy policy, which should be available to Data Subjects upon request. It should provide all relevant information about the data Processing.

Important grounds of public interest are triggered when the activity in question is part of a humanitarian mandate established under national or international law. This for example would be the case for the ICRC, National Societies of the Red Cross/Red Crescent, and other Humanitarian Organisations mandated under national or international law to carry out specific tasks, in so far as the Processing of Personal Data is necessary to accomplish those tasks. In this case, **the term "necessary" is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient).**

Cases where this legal basis may be relevant include distributions of assistance, where it may not be practicable to obtain the Consent of all the possible beneficiaries, and where it may not be clear whether the life, security, dignity and integrity of the Data Subject or of other people are at stake (in which case "vital Interest" may be the most appropriate legal basis for Processing).

Legitimate interest Humanitarian Organisations may also process Personal Data where this is in their legitimate interest, in particular, when a specific humanitarian activity is listed in their mission, and provided that this interest is not overridden by the fundamental rights and freedoms of the Data Subject. In all of these situations, the term "necessary" is to be strictly construed (i.e. the data Processing should be truly necessary, rather than just convenient, to fulfil the relevant purpose). Legitimate interest may include situations such as the following:

- The Processing is necessary for the effective performance of the Humanitarian Organisation's mission, in cases where important grounds of public interest are not triggered due to the absence of a mandate under domestic or international law.

- The Processing is necessary for the purposes of ensuring information systems and information security and the security of the related services offered by, or accessible via, these information systems, by public authorities, Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), providers of electronic communications networks and services and by providers of security technologies and services. This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems.

Compliance with a legal obligation. Under this legal basis, Humanitarian Organisations may process Personal Data where it is necessary to comply with a legal obligation to which Humanitarian Organisations are subject, or to which they submit.

Legal obligation as a basis for the Processing. These will be relevant in particular when authorities require access to Personal Data for law enforcement or intelligence purposes:

- existence of the rule of law and separation of powers in the country requiring access to the data;

- respect for human rights, including the right to effective judicial redress;

- existence of an armed conflict or a situation of violence, where the authority requiring access may represent a party;

- the nature of the data, and whether inferences could be made from the data leading to discrimination or prosecution (for example, if data relating to food needs reveal religious affiliation, if Health Data reveal sexual orientation in a country where homosexuals are persecuted, or if the Data Subject whose data are being requested faces the death penalty); and

- whether the Humanitarian Organisation enjoys privileges and immunities, and the obligation is not, therefore, applicable.

In this respect, it is also important to stress that Humanitarian Organisations should consider whether any legal obligation to disclose data applicable to them may put their Data Subjects at risk of repression, in which case they should consider not engaging in data collection in the first place.

- That data protection is a central part of the Red Cross Movement humanitarian mandate;

- The RFL CoC is a practical tool that assists NS to ensure that certain minimum standards are met, not only for RFL activities but indeed all NS activities that involve the processing of personal data, and which assists legal advisors to talk to their operational colleagues using common, Movement-familiar language to ensure data protection; the sections on informed consent, public interest and vital interest are particularly instructive in light of the humanitarian nature of the Movement's

activities and the CoC compliance checklist is a useful tool to further assist NS in strengthening their data protection;

- NS must only collect what they absolutely need and no more for a specific activity; they must ensure consent is informed, and ensure secure data management - all to mitigate risks to personal data;
- The need to protect beneficiaries' privacy and confidentiality is paramount, notwithstanding the pressure to produce ever more data including to show results;
- the RFL CoC relates to all Movement activities and not just RFL;

6.3 Child Protection Policy

The Red Cross Movement is committed to providing a safe environment for any child with whom it comes in contact, through implementing child-safe practices within its culture, programs and activities, policies and procedures. This Policy is to be known and understood by all personnel and implemented at all levels. The RC Movement is committed to ensuring that it, and anyone in contact with children in connection with the activities and programs of the RC, abide by national and international legislation relevant to child protection.

This responsibility falls upon all of our staff and representatives and is reflected across many policies. This duty of care is enshrined in our Child Safeguarding Policy.

7 Conclusion & Summary of recommendations

Given that the *ChildRescue platform* follows a tiered approach and it consists from multiple layers where personal data are collected, analysed or reported, data protection should be ensured at all levels before the platform become fully operative and for the piloting phase in at least Greece and Belgium.

To this end, the following actions are recommended to ensure in advance that ChildRescue R&D activities -including methods, tools, technologies and processes- comply with existing legal framework, ethical and privacy principles concerning access to personal information and data protection.

The following recommendations categorized under the four fundamental ethical principles are suggested to be taken into account:

1. ***The Principle of Beneficence*. ChildRescue should aim to bring about good in all its actions**; in this case special attention should be given in order to avoid direct conflict with respecting the autonomy of other involved parties.
    a. Acquiring National Data Protection Authorities' license for establishment and operation of register containing sensitive personal data. In this license should be clearly and detailed defined the purpose of the ChildRescue Platform and App concerning both, the primary and secondary uses of data to be collected and processed; the benefit of primary use of data is the investigation for finding a missing and/or unaccompanied child while the benefit of secondary use of data is about the sensitization of the community and activation of its sources towards supporting families in crisis and in particular towards the prevention of child disappearances and the more efficient management of cases of children declared as missing.
    b. All ChildRescue functions (including profiling methods, semantic extraction of tags, sentiment analysis, social network analysis, applying activity theory principles and predictive analytic methods) should target to identify the missing child; treatment of personal data of third parties (such as anonymous app users) should be appropriate for avoiding any violation in the agreed terms of use of the app.

2. ***"First, do no harm"-The Principle of nonmaleficence*. ChildRescue should undertake the obligation not to harm any of the involved parties** including **children** (missing and/or unaccompanied refugee and migrant children or to be traced); **guardians** (including parents/other legal guardians/tracing applicants); **professionals** (either who work with the cases such as psychologists, social workers, the police and pubic prosecutors or have administrative, operational or IT roles); and **platform users** (namely "community sensors", at various levels including registered identifiable users; register users and anonymous users).
    a. ChildRescue should respect the first principle concerning both, children who are the main platform's beneficiaries but indirect users and all relevant stakeholders who are platform's direct users and have the role of data sources and data administrators. To achieve this various techniques to ensure data privacy could be applied such as data anonymization; blockchains; pseudonymization; physical or digital restriction of access; and controlled (graded) access to data.
    b. Protection of privacy and personal data is a human right and any inappropriate use of these data can harm the subject of data; the ability, however, to protect privacy and personal data in the context of a platform or mobile application is a technical matter. Therefore, in order to ensure appropriate level of sensitive personal data protection and avoid harm application of *privacy design principles* (including data minimization;

controllability; transparency; user-friendly systems; data confidentiality; data quality; and use limitation) is recommended.

c. Providing that ChildRescue is dealing with children's data, it should be ensured that necessary standards and regulations are applied in order to prevent any misuse of application (as, for example, monitoring of data access; monitoring of various stakeholders/users actions; and ensuring that the system is well-protected).
d. Detailing step-by-step instructions for data sharing, real-time messaging and collaborative tagging is recommended to be included in Terms of Use for main investigators (national authorities, volunteer organisations and rescue teams) and Terms of Use for app Users.
e. Transparent administration of log files should be adopted regarding their content, protection, access and destruction; in other words it should be decided in advance what information is worth keeping in the context of ChildRescue, given the ethical risks of doing so.

3. ***The Principle of Respect for autonomy*. ChildRescue should respect the autonomy of involved parties**, namely to respect their decisions concerning the collection and use of their personal data according to what it was agreed per case.
    a. Subjects' of data (and missing children's legal guardians) should be adequately aware in advance for primary (*investigation for missing children*) and secondary (*profiling; identifying patterns; extraction of lessons learned; retrieval of similar cases*) use of their data, before they provide their consent for data collection and use. Informed consent forms as well as Terms of Privacy should include explicit information on this issue.
    b. Clearly described *Terms of Use* is recommended to be drafted (although it is not mandatory) concerning all groups of community users (registered identifiable users; registered users without personal identifiers; and anonymous users) and main investigators of the ChildRescue (national authorities, volunteer organisations and rescue teams) in order to ensure appropriate use of the platform and app during cases' investigation and to prevent misuse of the system or breath of confidentiality and data privacy.
    c. Personal data should be processed on the basis of the consent of the data subject concerned; in the investigation cycle for a missing or unaccompanied child, however, the main subject of data collection and processing (the child) is practically not feasible to provide his/her assent and therefore informed consent can be challenge and should rely to legal guardian of the child. Similarly to other systems/programs of communicating information of missing children (such as the Amber Alert) parental/legal guardian informed consent should be obtained before using child's personal data in the context of ChildRescue Platform and application, along with the permission of the Police (or other responsible authority). A standardized informed consent form is recommended to be developed on the basis of which missing child's parent/legal guardian will allow the use (upload and dissemination) of child's personal data through ChildRescue Platform and application.
    d. Acquirement of agreements with third parties (such as social media platforms) containing terms of cooperation is recommended; in the context of such agreements it should be clearly stated, for example, whether the third party service provider's terms of service and privacy policies govern ChildRescue users activity on the third party website or whether ChildRescue Platform intents to collect and maintain personal data the users make available on third party websites.

4. ***The Principle of justice*. ChildRescue should have an obligation to treat all people equally, fairly, and impartially**.

a. Clear definition of roles, rights and accountabilities of the users working in operating organisations should be the first step toward appropriate treatment of platform relevant stakeholders' personal data. Operating organisations should guarantee that ChildRescue platform and application comply with existing national and European data protection laws and regulations and that users' rights according to GDPR (such as easier access to their data; right to data portability; right to erasure or *'right to be forgotten'*; right to know when their personal data has been hacked) are respected.
b. Apart from the phase of the platform design and build, it should be ensured that during the pilot and, afterwards, the full operation phase ChildRescue will operate according to what provisioned by the law, ensuring in this way equal, fair and impartial treatment of all involved stakeholders.
c. Processing of personal data should also follow basic principles as they are referred in Art. 5 of GDPR including awfulness, fairness and transparency; purpose limitation; data minimization; personal data accuracy; storage limitation; integrity and confidentiality and accountability.
d. In cases that more than one countries are involved in an investigation (as, for example, in cases of international kidnappings or unaccompanied refugee and immigrant children) the legislation to be followed should be pre-decided.
e. The level of access of authorities requesting data (such as the IP address, the date, time and place they used the mobile app) of non-identifiable 'community sensors' (namely registered users without personal identifiers and anonymous users) should be clearly pre-defined in order to avoid any type of privacy violation and at the same time the Platform to operate according to the law.
f. **Privacy Policy:** ChildRescue is expected to collect, store, and share personal data (e.g. names, email addresses, IP addresses, location data etc.) of missing or unaccompanied children as well as of other groups of users. Therefore, an easily accessible privacy policy shall be drafted to inform users at least about what is ChildRescue; what personal data the app collect and process and why this is necessary; whether personal data will be disclosed to third parties and if yes, specifically to whom; and what are their (users') rights, in terms of withdrawal of consent and deletion of data. Drafting of a privacy policy is mandatory, as both the relevant directives are imperative laws.

Annex I: Templates

This Annex will contain the templates of the informed consent/ascent forms, information sheet policies etc. At this early stage of the project, these cannot be generated. The section will be completed during the update upon development of the informed consent and finalization of the rest documents.

Annex I: 26/04/2018 EAB Meeting Report

The ChildRescue Ethics Advisory Board (EAB) was formed and it includes experts in the field. Their names and positions are mentioned in the Table below (Table 3-1**Error! Reference source not found.**):

Table 3-1: The ChildRescue Ethics Advisory Board (names and position).

Name	Position
Philip Ishola (EAB Chair) (PI)	LOVE-146 international in human rights and technology
Karen Shalev Greene (KSG)	Director of the Centre for the Study of Missing Persons
Eva Lievens	Professor Specialised in Human rights and technology
Spiros Salamastrakis (SS)	Lawyer
Prof. Dr. Andreas Jud	Professor
Peter Van Dyck	Lawyer
Thanasis Giannetsos	Lecturer in Secure Systems
Antoine Bon (AB)	Legal advisor

The Board was sent, before the meeting, some relevant documents so that they can get to know the scope and the main aim of the project. Initially the Board members received a briefing document to prepare for their role in the project. After appropriate time was allowed for the EAB members to familiarise themselves with the project, further documentation was sent: The Draft deliverable D1.2, the Deliverable "D1.1. User requirements", the "Ethics Summary report", and the "Roles and Functions of Ethics Advisors/ Ethics Advisory Boards in EC-funded projects". The meeting took place on Thursday 26th of April 2018, at 15.00 to 17.00 CET. Attending the meeting were Philip Ishola, Karen Shalev Greene, Spiros Salamastrakis and Antoine Bon. From NTUA, the meeting was hosted by Christos Ntanos(CN), and Eleni Kanellou, Ariadni Michalitsi and Dimitris Varoutas kept the minutes and notes of the meeting. Further feedback on the report has been provided by the rest of the EAB members.

In this report the meeting minutes and some notes are given. In the meeting initially, a roundtable introduction of the members took place, followed by an introduction of the project and by questions that may have emerged, then the ethics requirements were presented and an EAB chair was appointed, finally a discussion about ethics related issues was held.

Meeting minutes

In this section the meeting minutes are quoted.

At first there was a roundtable introduction of the members of the EAB.

Then, CN introduced the ChildRescue project. When a child goes missing, and it is deemed necessary, a broadcast of the disappearance, either with Amber Alert or other means goes off. But many people might not receive it at all. There is insufficient capture and diffusion of information. Also, there is not a mechanism that integrates all available sources of information. Additionally, when a child goes missing, there are not any location-based alerts. The idea of social sensors is inserted in ChildRescue (citizens, volunteers, etc.) so that information about the location of a missing child can be provided or so that the tracking of the unaccompanied migrant minors is effective.

ChildRescue Investigation Cycle includes four main stages: Preparation, Coordination, Action, and Archiving.

Depending on the information ChildRescue gathers, the platform will predict the possible locations that the missing child might be at. As new information arrives, the radius will be getting smaller or bigger, depending on the information.

The idea of a mobile application is introduced. The application will be installed by the end users and notifications will be sent to them about the missing children, only if they are within the specific radius. In other words, the within the radius users will directly receive first-hand information.

One ChildRescue objective is to reduce the time frame between the moment children go missing to when they are found. ChildRescue will also increase social responsibility, as it will not only increase the effectiveness of the current search method, but it will also promote a certain sense of involvement of the general public in the missing children cases.

ChildRescue is currently on M4 of the total 36 months. Most of what is going to be needed when the platform becomes operational, e.g. data, has already been identified. But there will be an update on the piloting phase, e.g. some forms haven't been created, since the core methodology hasn't been described yet.

KSG asked about Childrescuealert from the UK and asked if ChildRescue partners are aware of it.

CN responded that ChildRescue partners are aware of it but haven't collaborated with them yet. The value proposition of ChildRescue is mostly the predictive algorithms.

CN highlighted that the system will be used by missing children organizations and that the information collection comes from parents, police, social workers of the organizations, volunteers, and

the private citizens. ChildRescue gathers information at the profiling stage either after a child's disappearance or in case of unaccompanied migrant minors, ChildRescue will gather information that might be of potential use in case of a disappearance, because unaccompanied migrant minors have higher probability to go missing. ChildRescue would like to know where they are or which is their target country, in order to act fast in case they do go missing. Missing children circle is the same for both cases but is initiated by disappearance in the first case and by an appearance in the second case.

Then, KSG asked about the profiling stage and the predictions.

CN said, for example the radius will be increased or decreased depending on the possible travel routes, e.g. in the hosting facilities, the social workers ask the unaccompanied migrant minors if they have a final destination. This is noted and if there is a flag that their life is in danger, or there is a tracing request, ChildRescue can use the information they have, and predict where the child might be. Moreover, in case of a parental abduction, and the parent leaves to another city, following the routes between the cities, ChildRescue could send alerts along that route. Although, many organisations will have access on the platform, each will have their own islet of information. Data from one organisation won't be shared with others unless they for some reason agree to do so. This is done due to data ownership disagreement between the organisations. A Pan-European network for that kind of data would be the next step, but the current framework doesn't allow it.

As far as the ethics self-assessment is concerned, the ethics issues were identified. For example, there are people unable to give informed consent. Additionally, ChildRescue won't keep any data, such as fingerprints, DNA, etc., but it will keep behavioural data. There will also be a secondary use of data, which will be done in the last stage of the investigation cycle, the Archiving. The proper way of deleting an Archive is to erase everything when the case is closed, i.e. when the child is found, when minor becomes an adult or when they are no longer in need of hosting facilities. There will be anonymization (the method hasn't been decided yet) and aggregation of the data.

The police won't be directly involved in ChildRescue. The information sharing with the police can be done indirectly, if deemed necessary.

CN clarified that the information that is going to be shared between the missing children organisations and the public, will not be different than the current information that is shared in the case of an Amber Alert. But more information will be given to specific volunteer groups involved in the investigation.

Instant messaging was also an identified ethics issue. Citizens can only message members of the missing children organizations. Additionally, the caller's right to anonymity will be integrated in ChildRescue.

There were also some disagreements with the ethics review such as: 1. the burden of the potential harmful uses of the platform must fall on the developer/owner, not the user and 2. the app will allow for users to register anonymously. While their public identity can be anonymous, police forces should always be able to identify who is providing evidence that is related to an open case. The

organizations allow citizens to anonymously call and this is generally accepted by the police. The anonymity is protected, although the IP and MAC address, might be available through log files.

What ChildRescue did, was to define the 12 specific requirements on the identified categories of the project. The ethics deliverable will be given by the end of this year and there will be a couple of updates; one in the interim review on M15, and one at the end of the project on M36.

CN briefly described the ethics requirements.

SS said that the problem is about the data protection and ownership.

AB noted that the only thing that matters is who decides what to do with the data, i.e. who is the data controller - data protection officer (DPO) of the organization. The data controller is the person/authority/agency which ALONE or JOINTLY (see art. 26 GDPR) with others, determines the purposes and means of the processing of personal data (art. 4, 7° GDPR). The role of data controller entails a series of obligations (Chapter IV GDPR). This role is different from the data protection officer role who in certain cases should be appointed by the data controller (art. 37 GDPR) and carries not responsibility for the processing. The location itself does not have any impact. SS said that the organizations must have a data protection officer by the 25th of May 2018.

CN gave an example of a DPO, that collects the personal data for an organization and wandered if that is the same as the person who decides to send some information to the police (phone, fax, email) as will be done by ChildRescue. CN also wandered if there is any other special requirement that should be covered.

PI responded that this may not be an ethical question, but there should be a clear cleaniation of the mechanisms that define the sharing of information. There is no problem with the case of being the same person, but it is better if the person is differentiated. It should be a very clear line as it is a separate process. The coming in and coming out data streams should be separate and housed as such.

AB suggested ChildRescue to create a scheme of the different actors, data controllers, coc controllers, etc., in order to understand the data flow. CN said that he will translate this into an actual requirement based on the WP of the project. So, a list will be created that connects the GDPR actors and the already identified actors from the D1.1.

KSG wanted ChildRescue to clarify which are the relevant information and what ChildRescue does with them after the case is closed.

CN replied that after a case is closed, data pseudonymisation is done. Possible reopening of certain cases could be done. ChildResque is considering the idea of a safe of information, where no one will have access, except after granted special permission. The specific key by which a case is encrypted, will be removed or substituted by another key, locking the safe until there is a special request for any case to be reopened. That's one idea of not completely deleting the data but keeping a small window for the possibility that there may be a need to reopen the case after a request. If someone requests

to delete the case, the idea is to throw away the key completely. CN asked if throwing away the key is enough for the right to be forgotten?

CN said that information is collected, from the forms that missing children organizations already use, e.g. to gather information from the parents, etc. Because organisations have a lot of forms and a lot of information is repeated, aggregation is very important. In terms of which information ChildRescue collects, at least at this stage, there nothing more of what is already collected.

KSG asked what ChildRescue does with the material that is not relevant? CN responded that the project is not a platform to keep lists of cases. ChildRescue won't provide a system to run algorithms or a data analysis. You can't know which information is relevant or irrelevant if you don't know the conclusion of the case.

PI said that holding information is actually quite important for analytical purposes that relate to trafficking modus operandi or vulnerability spots in migration routes as long as the criteria for usage of personal information is clearly set out at the start. The holding of personal information for undefined purposes involves risks. Anonymised personal information would require a different classification, as personal details would no longer be identifiable.

AB said for the case of anonymisation, that is mainly out of the scope of GDPR, because when the anonymisation is done correctly then the data are no longer considered personal, but ChildRescue needs to find the most appropriate way of anonymisation.

CN asked if someone encrypts data in such a deep level, that the data cannot be restored without the key and you delete the key, are the data considered deleted? SS replied that a hacker could steal, unlock and retrieve the data.

CN said that there will be a unified database and different organizations will have access to specific parts of the database. A good idea for handling parts of the data is blockchain; it contains all the transactions that happen. There is a high possibility to use blockchain for the communications, but not for the case files.

AB said that even if someone encrypts the data and throw away the key and a hacker retrieves the data and there is a link between the data and the individual, then there is a serious problem. The link between the data and the individual should be removed.

Finally, ChildRescue should have complete control of the data deletion. The data and the logs should be purged.

Notes

In this section some notes that conclude the issues that were discussed are presented. Some of those issues are: the implications associated with research on humans and the handling of the sensitive personal data.

One of the implications regarding personal data is who will be in charge of handling them, thus also ensuring their safety. Usually, the controller of the data is considered to be the organisation that gathers all the information. In our case, this can be a little tricky since there are more than one organisations involved. Thus, the question of who is responsible for data security emerges. Initially, whether the location that the data are gathered and stored is an issue was mentioned. The Board explained that the geographic location of the data (since in any case this location will be within the EU) does not really matter. In fact, there is no such thing as an "owner" of the data, but rather who has the responsibility of securing them. Usually there is a person charged with this task and is called a data protection officer or controller. Effective 25th of May 2018, organisations will be required to appoint a DPO, the designation of whom is only mandatory in certain cases (art. 37, 1° GDPR).

At the same front, the issue of the dissemination of information in case of an emergency was discussed, e.g. if SoC decides to send some information to the police in a form of a report. According to the Board this would not necessarily be an ethical issue. It mainly depends on the processes that are followed. There is the need of the existence of clear mechanisms, because the streams of information may be coming from various sources and that is usually the case when different information are gathered in the same report from different organisations. GDPR clarifies that there needs to be some kind of mechanism handling the streams but also a separate security code. Maybe some kind of scheme could be in place that involves different actors. There also needs to be clarity as far as GDPR is concerned. Bottom line is that a list or a diagram that connects the already in place actors with the already identified stakeholders needs to be drafted so that the roles could be presented as outlined in GDPR.

Another issue that emerged is how to handle the data if there are excessive information, that may no longer be needed, or if the case is closed and there is the need to delete all the related information. In any case, a pseudo-anonymisation takes place, so that there will be an archive of cases if ever there is a need to reopen a file. The idea that maybe there will be some kind of a safe for information was discussed. Another idea is to encrypt the information and to protect them with a "key" that will be removed or destroyed after the case is closed, and the organisation in charge will shield the data unless it is absolutely necessary for them to be reopened. In case of a request to delete everything (e.g. the child that the case is about wants the data destroyed when an adult) then the key will be "thrown away". As for the kind of data that will be collected, they will be no different than the data that both Smile of the Child and Red Cross are currently gathering. Regarding the material that is gathered but may not be relevant, the approach followed will be similar to this of big data analysis and it will mainly include eliminating the noise. Also, there is no way to know which information will be irrelevant until the conclusion of the case. What was outlined as of extreme importance is that the data should not by any means be traced back to individuals. That is why the idea of using blockchain technology was discarded.

What is more, another issue that was raised, is that when the data have already been anonymised then different handling is needed for the data that are personal and will be kept stored. If the data have to be deleted, problems could emerge if there is not a clear framework and very secure mechanisms. This is something that goes out of the scope of GDPR. Maybe there is a need to validate the mechanism of anonymization, however, GDPR is technology neutral so the choice of the method

is free but it needs to take into account the risks involved. Thus, it is important to find an anonymisation technique that is suitable for each case.

Furthermore, the national technical authorities were mentioned and the need for them to greenlight the project now, so that when the pilot is ready it can be launched. The EAB members highlighted that the respective authorities do not greenlight projects. According to the Greek Law each Data Controller is required to notify the Authority of the establishment and operation of the Data or of the processing to the Hellenic Data Protection Authority. This procedure is called "notification - application for licence". As for Belgium, there is a Privacy Commission but is not entitled with the task of "greenlighting" projects. Also, the ICO in the UK does not greenlight anything either, there is a need to register there, especially when using personal data for specific purposes but inspection and compliance function is within the scope of ICO's activities.

Finally, the EAB concluded that a scheme suitable for ChildRescue should cover the matters mentioned below:

The different actors and their roles under the GDPR (controller – Processor – joint controller).

The data flows between the actors and the purposes for which the data is exchanged.

The lawful basis for processing for each of the processing (art. 6 GDPR).

The type of data that will be processed (regular data or special categories of data under article 9 or 10GDPR).

The occurrence of profiling (art. 4, 4° GDPR) should be mentioned.

Directive 2016/680 may need to be taken into consideration when cooperation with the law enforcement authorities is necessary.