MIRAD

Multi-Ideological Radicalisation Assessment towards Disengagement

D5.6 – Recommendation paper towards the (implementation of) (EU) Directive 2016/680 and beyond

Author Names:

Luís Matos, IPS_Innovative Prison Systems

Raquel Venâncio, IPS_Innovative Prison Systems

This project was co-funded by the European Commission's Internal Security Fund – Police.

D5.6 Recommendation paper towards the (implementation of) (EU) Directive and beyond

Deliverable number	*D5.6*	
Deliverable Name	*Recommendation paper towards the (implementation of) (EU) Directive 2016/680 and beyond*	
Work Package	*WP5*	
Version	*0.5*	
Keyword list	Directive 2016/680; Data Protection Law Enforcement Directive; Data protection	
Licensing information	*Where relevant, for public documents*	
Contractual Date of Delivery	*Delivery date from DoA: M18 (as per amendment approved on the 23rd of March 2023)*	
Actual Date of Delivery	M18	
Type:	*Please choose only one of the types below:* - **R**: Document, report (excluding the periodic and final reports)	
Dissemination level:	*Please choose only one of the levels below:* - **PU:** Public	
Classification level	Unclassified	
Status	*Please choose only one of the statuses below:* - Draft	
Main author(s)	Luís Matos Raquel Venâncio	IPS_Innovative Prison Systems
Contributor(s)	Pedro Liberado Joana Apóstolo Markos Shangoyan	IPS_Innovative Prison Systems IPS_Innovative Prison Systems KMOP-Social Action and Innovation Center
Disclaimer	This document reflects only the author's views and not that of the Research Executive Agency. The Research Executive Agency is equally not responsible for any use that may be made of the information contained in this document. This document may not be reproduced or copied without permission. 	

DOCUMENT CHANGE RECORD

Version	Date (DD/MM/YY)	Status	Author(s), reviewer	Description
0.1	16/06/2023	Draft	Luís Matos (IPS), Raquel Venâncio (IPS), Pedro Liberado (IPS, reviewer)	Initial Draft shared with the Consortium
0.2	26/06/2023	Draft	Luís Matos (IPS), External Expert (reviewer)	Initial Draft reviewed by an external expert on FD 2016/680 and later adapted in accordance
0.3	07/07/2023	Draft	Luís Matos (IPS)	Added information in line with the International Policy Roundtable
0.4	11/07/2023	Draft	Markos Shangoyan (KMOP)	Draft reviewed.
0.5	04/08/2023	Draft	Raquel Venâncio (IPS), Pedro Liberado (IPS), Luís Matos (IPS)	Added information according to the last revision.
1	25/08/2023	Final version	Jeanne Dubroca (Cnam)	Formatting and submission.

Contents

List of Tables 5
Glossary/Definitions & Acronyms/Abbreviations 6
Executive Summary 7
Introduction 8
Work Package Overview 9
Structure of the Recommendation Paper 9
1. Data Protection Law Enforcement Directive | Scope of Application 11
Personal Scope 12
Material Scope 13
2. Data Protection Principles under LED 15
Lawfulness and fairness of the processing of personal data 15
Purpose limitation 16
Data Minimisation 16
Data Accuracy 17
Security and Confidentiality 19
Transparency 19
3. Obligations of the Controller under LED (see annex III) 19
4. LED in the context of MIRAD and necessary relation to GDPR 22
5. Differences between GDPR and LED 23
6. Practical Outlook from Field Experience 24
What are the main challenges you can identify in complying with LED while ensuring effective information sharing and collaboration among agencies? 24
How can inter-agency cooperation be enhanced to ensure efficient sharing of information while still upholding privacy rights and data protection principles? 25
Conclusions and Recommendations 26
Summary 26
Recommendations 27
References 29
Annexes 33
Annex I – Flowchart on right to access. 33
Annex II – How to respond to information requests. 34
Annex III – Data Protection Obligations 34

List of Tables

Table 1: Glossary/Definitions & Acronyms/Abbreviations

Table 2: Key differences between GDPR and LED

Table 3: Flowchart on the right to access

Table 4: How to respond to information requests

Table 5: Data Protection Controler Obligations

Glossary/Definitions & Acronyms/Abbreviations

Term/acronym	Definition / Description
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CSO	Civil Society Organisation
D	Deliverable
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
IPR	International Policy Roundtable
LED	Data Protection Law Enforcement Directive
MS	Member State
MIRAD	Multi-Ideological Radicalisation Assessment towards Disengagement project
NGO	Non-Governmental Organisation
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the European Union

Table 1 - Glossary/Definitions & Acronyms/Abbreviations

Executive Summary

The present Deliverable (D5.6 Recommendation paper towards the (implementation of) (EU) Directive 2016/680 and beyond) integrates Work Package 5 (Interinstitutional collaboration models and protocols towards effective disengagement and successful social reintegration) of the Multi-Ideological Radicalisation Assessment towards Disengagement (MIRAD) project. In this line, this recommendation paper provides a comprehensive analysis of Directive 2016/680, otherwise known as the Data Protection Law Enforcement Directive (LED). Through this, the present document demarcates LED's scope of application and puts forward important measures to facilitate compliance with data protection concerns. Primarily focused on the action of prison and probation officers, judges, magistrates and policy and decision-making actors, the paper also integrates holistic guidance directed at CSOs and NGOs, as well as valuable information for researchers and academics. Consequently, this deliverable promotes the compliant and effective processing of personal data, including data transfers (inter)nationally towards full respect of suspects, victims, witnesses and other relevant parties' rights.

Finally, it bears noting that the paper was drafted on the basis of an expansive interpretation of the concept of "public security" integrated within LED. This is a position widely reflected in recent reports of the European Commission on the topic, from which we highlight the "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680". In this, it is worth considering that the recommendations herein present are designed to comply with legislation at the EU level and may need further integration into national legislative systems. Such poses significant relevance when considering that LED is under the principle of minimum harmonisation, thus subject to a certain degree of national legislative deviation.

Introduction

Prisons have long been recognised as conducive environments to the emergence of violent extremism and radicalisation. In actuality, as highlighted in the European Union (EU) Terrorism and Situation Trend Report, prisons continue to provide pathways for radicalisation (EUROPOL, 2023). On one hand, prisons expose individuals to isolation, wherein intrinsic vulnerability exponentially increases the susceptibility of persons to exploring new relationships, beliefs, and identities. Similarly, individuals convicted of terrorism or extremist offences, under prison sentences, interact with *ordinary* offenders, thus posing a significant threat and increasing the risk of radicalisation (EUROPOL, 2023). Additionally, the role of prisons as a breeding ground for radicalisation has been widely highlighted, both by academia (e.g.,; Martins & Ziegler, 2018; Neumann, 2010) and multilateral international organisations (e.g., Council of Europe, 2016; European Commission, 2020). Amongst others, and as highlighted by Radicalisation Awareness Network (RAN, 2016), the prison environment can be favourable to inmate recruitment and support for extremist groups from (and within the) prison (EUROPOL, 2023). As a response, implementing a comprehensive and well-structured holistic approach to managing radicalised offenders at all stages can contribute to reducing recidivism, the spread of radicalisation and the resulting violent extremism across Europe.

In light of this, comprehensive strategies for rehabilitation (focused on deradicalisation) and reintegration have been put into place by several EU Member States (MS) to mitigate these risks, as acknowledged by various European institutions, agencies, and international bodies (e.g., RAN, 2019; Abrunhosa et al., 2020). In recent years, the EU has promoted a multidisciplinary approach involving policymakers, first-line practitioners in prison and probation authorities, social workers, educators, and experts from civil society and community organisations (European Parliament, 2018). Herein, the EU's Counter-Terrorism Agenda aims to combat terrorism and violent extremism by coordinating efforts among MSs, engaging European institutions, and involving society as a whole: citizens, communities, faith groups, civil society, researchers, businesses, and private partners (European Commission, 2020).

While many experts support the need for multi-agency cooperation in managing radicalised offenders, significant improvements are still needed in the field. Challenges such as lack of trust, limited access to specialised training, privacy concerns, and the absence of formal cooperation protocols and specific regulations continue to hinder the multi-agency approach to rehabilitation and reintegration across the EU. Given the lack of clarity at the EU level, and the lack of attention awarded to LED in lieu of the General Data Protection Regulation (GDPR), data protection emerges as a contentious topic that can hinder effective collaboration and the efficient functioning of specific protocols and programmes (Sajfert & Quintel, 2017). This becomes bleaker when considering the nuanced distinction between national and public security, for the purposes of delineating the Union’s competences, and the integration of extremism and terrorism prevention therein.

Against this backdrop, the present recommendation paper deploys a legislative, jurisprudential and literature review methodology to identify, to the extent possible, the scope of application of LED. Through this it is possible to identify best practices and measures to adopt in light of the applicable legislative documents, ultimately resulting in a list of comprehensive recommendations for policymakers and competent authorities alike. The document also provides practitioners with comprehensive practical guiding charts, aimed at facilitating compliance with data protection concerns. Through this, our recommendation paper aims to enhance fluid data sharing amongst competent public authorities (e.g., judicial authorities, the police or other law-enforcement authorities, but also any other body or entity

entrusted by MS law to exercise public authority and public powers for the purposes of this Directive, such as prison and probation general directorates). Lastly, following up on the practical learning tools and programmes, directed to NGOs and CSOs, developed in the context of the MIRAD project, with the aim of capacitating these actors, the present paper includes specific recommendations related to the transfer of personal data to third parties not integrated under the scope of application of LED. Hence, and by integrating another level of compliance and protection within their activity, it is possible to enhance the trust in these organisations, ultimately fomenting holistic collaboration.

Work Package Overview

The inconsistent use of radicalisation risk assessment tools in the process of offenders' rehabilitation practices has been identified as a major barrier to their successful reintegration into society. The progress made during their time in prison can easily be undermined if not adequately supported by subsequent agencies such as probation services and community organisations. Therefore, it is crucial to ensure cooperation and dialogue among various agencies to ensure a coordinated and integrated response. Recognising the limitations of the current inter-agency collaboration in rehabilitation and reintegration programmes, MIRAD's WP5 focuses on designing and promoting models and protocols for cross-sectoral and interinstitutional collaboration. These address the specific need for a seamless transition of offenders from prison to probation and their full reintegration into society. As such, they establish a framework for agencies to adopt a comprehensive cooperation mechanism in assessing offenders' risk of radicalisation and vulnerability during disengagement programmes. WP5 aims to strengthen the application of radicalisation risk assessment procedures in a comprehensive and long-term perspective, involving all relevant governmental agencies and institutions with the support of community organisations.

To this effect, WP5 is sub-divided into the following activities:

- **A5.1. Protocol screening and mapping of national and European collaboration strategies** – aimed at mapping existing protocols, as well as national and European collaboration strategies, integrated within relevant agencies involved in rehabilitation and reintegration programmes;
- **A5.2. Multi-agency and interinstitutional needs assessment** – directed at determining the efficiency and productivity of the existing inter-agency collaboration strategies and legislative initiatives vis-à-vis fluid transition processes towards social reintegration of radical offenders;
- **A5.3. Design of transition collaboration protocol baselines** – dedicated to the structural, methodological and operational conceptualisation of transition and collaboration protocols, so to facilitate and promote their subsequent adoption;
- **A5.4. Policy Roundtables towards protocol establishment** – organised to sensitise practitioners towards the importance of integrated, transversal approaches when activating individual rehabilitation programmes from VE, therefore longitudinally assessing the individual risk of radicalisation across the whole rehabilitation process; and
- **A5.5. Recommendation paper towards respecting the (implementation of) (EU) Directive 2016/680 and beyond** – dedicated to the integration of MIRAD's main concerns within the realm of data protection, providing therein comprehensive guidance towards compliance and full respect for the fundamental right to privacy and data protection.

Structure of the Recommendation Paper

This document comprises the following sections:

Section 1 – provides a comprehensive analysis of the scope of the application of Directive 2016/680.

Section 2 – includes a practical overview of the most relevant data protection principles considering Directive 2016/680.

Section 3 – explains competent authorities' obligations under LED.

Section 4 – provides a holistic integration of the topic of data protection within the realm of MIRAD's action.

Section 5 – comprises a summary of findings and a practical list of recommendations.

Section 6 – offers practical schematic guidance on competent authorities' action, namely with regard to the respect for the right to access, right to information and controller obligations under LED and GDPR.

1. Data Protection Law Enforcement Directive | Scope of Application

Part of the European Union's (EU) Data Protection Framework, the GDPR and LED are EU legal instruments aimed at safeguarding the respect for the right of data protection as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (Charter) and Article 16 of the Treaty on the Functioning of the European Union (TFEU). Stemming from the right to privacy, data protection developed as a branch of law dedicated to safeguarding fair, ethical, and respectful processing of personal data by public or private entities. **More concretely, the objective is to protect any information linked to an identified or identifiable natural person**.

In this line, LED was envisioned with the prime objectives of ensuring a high level of respect for fundamental rights in the areas of Policing and Criminal Justice and improving the transfer of personal data between MSs, thus covering the activities of competent authorities for prevention, investigation, and prosecution purposes of criminal offences (COM(2022) 364 final). In this, LED emerges as the first horizontal instrument covering both cross-border and domestic processing of personal data for criminal law enforcement purposes (Marquenie, 2017). In fact, as recognised under Declaration 21 to the TFUE, defining specific rules for the protection and free movement of personal data in the area of judicial cooperation and law enforcement activities is necessary, especially considering the particular nature therein. Through the safeguard that the personal data of suspects, victims and witnesses of criminal offences is duly protected, LED presents itself as a crucial document within the EU's security policy, and more concretely to the Area of Freedom Security and Justice. In parallel, by harmonising the norms that govern competent authorities' data processing in EU and Schengen countries, LED ensures increased trust and security when referring to data transfers between authorities, hence enabling cross-border cooperation in the fight against crime and terrorism (COM(2020) 797 final).

Contextually, it bears mentioning that LED's scope is circumscribed to a particular set of purposes and actors as defined in Article 1 thereof. As such, it bears mentioning that not all personal data processed by competent authorities will fall within the scope of LED. Consequently, "[w]here personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply (…)" (Article 9 LED).

Recommendation

Competent authorities should start by analysing their processing activity and assess if it fits within the scope of application of LED.

Article 1 LED states that "[t]his Directive lays down the rules relating to 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". From this, it is easily discernible that LED's application is dependent on a set of cumulative criteria, namely:

1. LED regulates acts whereby personal data is processed;
2. By competent authorities (Personal Scope);
3. For the purposes of 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 (Material Scope).

In line with Article 3(1) LED and Article 4(1) GDPR, "**personal data**" is to be understood as any information relating to a data subject. This data subject is a natural person identified or identifiable, directly or indirectly, by reference to a distinguishing marker (e.g., "a name, an identification number, location data, an online identifier or any marker linked to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person").

Following Opinion 4/2007 on the concept of personal data, to determine if a piece of information is "personal data" for the purposes of GDPR and LED, one should consider objective (unbiased) and subjective (qualified/biased) information, irrespective of the medium or format, that relates, concerns or is likely to have an impact on a natural person (the data subject), directly or indirectly identifies said data subject, and/or allows for his/her/their identification, considering all the reasonable means likely to be used either by the controller or a third person. In fact, as clarified in *Peter Nowak v. Data Protection Commissioner* (CJEU C-434/16; para. 34) "[t]he use of the expression 'any information' in the definition of the concept of 'personal data' (…) reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject". In what concerns the relation to the data subject one should consider if the content, purpose, or effect, of the specific information is linked to a concrete data subject (para. 35).

As provisioned under Article 3(2) LED and Article 4(2) GDPR, "**processing**" should be understood as including a myriad of operations performed on personal data, be it through manual or automated means (*inter alia*: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data).

Personal Scope

As above-mentioned, LED only applies to data processed by competent authorities. These actors should be considered a data controller – *i.e.*, an entity that either alone or jointly with others, determines the purposes and means of the processing of personal data (Article 3(8) LED). Under, Article 3(7) LED "**competent authorities**" include:

a) "any public authority competent for 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"; or

b) "any other body or entity entrusted by [MS] law to exercise public authority and public powers for 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".

Herein two categories clearly surface, namely **competent authorities *stricto sensu*** and **entities assigned law enforcement tasks by national law** (Brewczyäñska, 2022). While the former seems to fall strictly under the field of criminal justice, the latter appears to open LED to a broader scope of applicability (Vogiatzoglou & Fantin, 2019). In this, due to the extended personal scope of the application LED provides, which reaches beyond traditional law enforcement authorities, establishing a clear border between LED and the GDPR becomes ever more difficult (Caruana, 2019).

Competent Authorities Stricto Sensu

LED requires competent authorities, under Article 3(7)(a) thereof, to be public. This characteristic is, in principle, attached to public ownership (Bozeman & Bretschneider, 1994) – *i.e.*, the level of public funding or the degree to which an organisation and its activity are subject to public regulation. Having established the publicness of the entity, one should then look at its competence "for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (infra explored in the 'Material Scope' section). Under Article 2(a) of the EUROPOL Regulation, competent authorities are defined as "all police authorities and other law enforcement services existing in the MSs which are responsible under national law for preventing and combating criminal offences". Consequently, examples of competent authorities may be police forces and public prosecution services, judicial magistrates, prison facilities, juvenile correction centres, forensic psychiatric centres, and probation authorities (recitals 11 and 22 LED).

Entities Assigned Law Enforcement Tasks by National Law

The expansion of the legal definition of a competent authority beyond its strict sense was proposed by the Council (Council of the European Union, 2016). This position was never formally explained, thus allowing for some speculation as to its meaning and scope.

Unlike the competent authorities *stricto sensu,* these other entities do not need to be public, hence encompassing private organisations, as long as legally entrusted with the competences to act with public authority and public powers for the purposes of law enforcement. It should be highlighted that the use of the conjunction "and" effectively makes the entrustment of **public authority** and **public powers** a cumulative criterion, hence narrowing the scope of application of this provision. In this line, Article 3(7)(b) can be read as covering the odd scenario wherein **the State privatises its law enforcement activities, for instance, the existence of private prisons functioning in the United Kingdom** (Purtova, 2018).

Given the undefined nature of the concept, **it would be valuable for MSs to maintain a list of entities considered "competent authorities" for the purposes of LED**, similar to the one provisioned under Framework Decision 2006/960/JHA, Article 2(a). Such a centralised list would not only clarify emerging doubts as to the scope of LED, but also ensure legal certainty and facilitate cooperation (Brewczyäñska, 2022).

Recommendation

MSs should maintain a list of entities considered "competent authorities" for the purposes of LED.

Material Scope

As provisioned under Article 1 LED, read in conjunction with article 2(1) thereof, the Directive merely applies to data processing "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".

Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties

Contextually, LED details 5 law enforcement purposes, which bring the processing of personal data under its scope. In this, "**investigation**", "**detection**" or "**prosecution** of criminal offences" and the "**execution**

of criminal penalties" represent the different stages of the criminal proceedings (*i.e.*, pre-trial stage, prosecution, and execution of a sentence, respectively) (CJEU C-180/21, para 42). It bears noting that *de facto* court proceedings are thus excluded from the material scope of this directive, which "does not preclude [MSs] from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings"(Recital 20 LED). Irrespectively, the lack of specificity in the instrument awards MSs with a certain degree of flexibility in their transposition. This phenomenon is exacerbated when considering that law enforcement activities are generally subject to national law and will consequently differ from MS to MS.

On the topic of "**prevention**" – *i.e.*, "efforts to prevent crime or criminal offending in the first instance – before the act has been committed" (Welsh & Farrington, 2012) –, the numerous manners in which States can pursue this purpose make it hard to concretely delineate its extent. **In so far as applying specific data protection rules proves necessary, proportionate, and justifiable LED may apply**. Similarly, the intrinsic differences in regulation at the State level render the objective of harmonisation and cooperation harder to achieve.

Criminal Offence

LED does not define the term "criminal offence", merely stipulating in its Recital 13 that it should be understood as an "autonomous concept of Union law as interpreted by the Court of Justice of the European Union". In considering the lack of clear definitions on the part of the Court of Justice of the European Union (CJEU), one may rely on the European Court of Human Rights' (ECtHR) **"Engel criteria"** for clarification. The "Engel criteria" establishes 3 conditions to define "criminal offence", namely: (1) classification of the offence under domestic law; (2) the nature of the offence; and (3) degree of severity of the penalty that the person concerned may incur (ECtHR, Engel and Others v. the Netherlands, para. 22).

Safeguarding against and the prevention of threats to public security

Added by the proposition of the Council (Position (EU) No 5/2016 of the Council), this phrase appears to expand the already rather broad meaning of law enforcement tasks covered by LED, effectively allowing MSs to further deviate from the narrow understanding of the role, objectives and needs of criminal law and criminal proceedings that justify the existence of specific data protection regime. Recital 12 LED explains that relevant action undertaken by law enforcement authorities may include "maintaining law and order as a task conferred on the police or other law enforcement authorities where necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence". In this, the data processing under LED may diverge from the core notion of "criminal offence", and thus the nucleus of law enforcement.

Contextually, and for the purposes of MIRAD, it merits noting that under Recital 14 and Article 13(3)(d) LED clearly demarcates a border between "Public Security" vs. "National Security". This stems from the fact that LED is "intended to contribute to the accomplishment of an area of freedom, security and justice" (Recital 2 LED) rather than the common foreign and security policy. Union law often resorts to the term "national security" so as to define the limit of its competences and regulatory powers, nonetheless, it has failed to provide a clear definition (Vogiatzoglou & Fantin, 2019). The expression has conventionally been linked to sovereignty and to the democratic nature of the state, a vision echoed in Public International

Law. As such, "national security" has traditionally encompassed, amongst others, terrorism. Simultaneously, however, in the EU, "public security" has evolved as an ever-expansive autonomous concept, used to justify EU policy in general, and counter-terrorism action in particular. Consequently, secondary legislation and CJEU jurisprudence have effectively widened the scope of the term to include domains that are usually seen as being under "national security". For the purposes of LED, this approach seems to be echoed in the European Commission's "First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680" (COM(2022) 364 final). The paradox emerging from this overlap raises several questions as to the scope of the application of LED. One could infer that "public security" might be as broad as covering both the internal and external security of the MS, public safety, societal security, survival of the population and peaceful coexistence of states.

2. Data Protection Principles under LED

Recommendation

National Law should clearly define data protection and LED specific terminology. Herein, concepts such as criminal offence, public security, national security, competent authority, should be the subject of comprehensive clarification that follows European law and jurisprudence.

Recommendation

MSs should clearly define the types of activities included under the umbrella of national security, thus delineating the actions covered under article 4(2) of the Treaty of the European Union, which are in turn excluded from the scope of LED.

Lawfulness and fairness of the processing of personal data

In line with Article 8(2) of the Charter, and following *Schrems II* personal data should be processed "for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" (CJEU C-311/18, para 173). Nevertheless, within law enforcement, it ought to be highlighted that the tasks of preventing, investigating, detecting, or prosecuting criminal offences, legally conferred to competent authorities, provide them with the ability to require or order natural persons to comply with specific requests. As such, within LED, the **consent of the data subject is not suitable to act as a legal ground for processing personal data by competent authorities** (EDPB, 2021).

In this, and following the above exposé, it is important for a legal basis to be clearly laid down in precise norms that both define the scope and application of the relevant data processing activities and impose minimum safeguards (CJEU C-311/18, paras. 175 and 180). To be lawful, data processing should be regarded as necessary for the performance of the task carried out by the competent authority (EDPB, 2021). **In this, the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security should be provisioned within national law**. Amongst others, this ensures legal certainty at the national level. **Consequently, personal data must be obtained and processed lawfully and fairly**.

Finally, it bears noting that fair processing differs from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (Recital 26 LED).

Recommendation

The purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security should be provisioned within national law.

Recommendation

Personal data must be obtained and processed lawfully and fairly.

Purpose limitation

Prior to the collection of data, the specific purposes for which personal data is processed should be explicitly and legitimately determined. **In this, any processing should clearly identify a specific, unequivocal purpose within the realm of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security** (CJEU C-180/21, para 50)**.** If personal data is to be processed by the same or another competent authority for the purpose of preventing, investigating, detecting, or prosecuting criminal offences or executing criminal penalties other than that for which it was collected, considering it is legal, necessary and proportionate, such processing should be allowed under LED. Following, implementing **mechanisms, such as mutually agreed handling codes, notification obligations or other transparency measures, could inform the relevant competent authorities of further processing**. Irrespectively, the **level of protection awarded to data subjects by LED should not be undermined**.

Recommendation

Processing activities should clearly identify a specific, unequivocal purpose.

Recommendation

Competent authorities should implement mechanisms, such as mutually agreed handling codes, a notification obligations or other transparency measures, to keep track of processing conducted by other entities.

Data Minimisation

Processed personal data should not be excessive and should be adequate and relevant. *In concreto*, Competent Authorities should **resort to mechanisms of data protection by design and by default.** Similarly, personal data **should not be kept for more than what is deemed necessary for the purposes for which it is being processed.** To this effect, competent authorities should put in place **appropriate mechanisms for the erasure of personal data, for instance by establishing periodic reviews of the**

necessity for storage of personal data. If deemed relevant to store personal data for longer periods of time, due to public interest, scientific, statistical or historical value, it should be subject to appropriate safeguards (Recital 26 LED).

Recommendation

Processed personal data should not be excessive and should be adequate and relevant. It should not be kept for more than what is deemed necessary for the purposes for which it is being processed. In this, competent authorities should put in place appropriate mechanisms for the erasure of personal data, for instance by establishing periodic reviews of the necessity for storage of personal data.

Data Accuracy

Personal data should be maintained in an accurate and up-to-date manner, without prejudice to the necessary considerations of the nature and purpose of processing. For instance, within the context of judicial proceedings, personal statements are subjective and not necessarily verifiable, in this scenario accuracy solely refers to the fact that a specific statement was made, and not necessarily to the rigour of its content. Similarly, **mechanisms should be implemented to safeguard that inaccurate data is not transmitted or made available and to ensure its subsequent deletion or correction.** In this, the European Data Protection Board has identified the usefulness of classification systems of data as to the reliability of source and fact verification level – e.g., 4x4 grids for reliability assessments and handling codes (EDPB, 2021).

Recommendation

Personal data should be maintained in an accurate and up-to-date manner, without prejudice to the necessary considerations of the nature and purpose of processing.

Recommendation

Safeguards should be implemented to ensure that inaccurate data is not transmitted or made available and facilitate subsequent deletion or correction.

Right of Access, to Rectification and Erasure

In the context of competent authorities' duty to ensure data accuracy, the data subject has a **right to obtain confirmation on the existence of processing activities concerning his/her/their personal data**, in which case he/she/they have the **right to access said personal data**. This should be accompanied by **information on purpose, category of personal data, disclosure, storage period, existence of request for rectification or erasure, right to lodge a complaint and source of data** (see flowchart in annex I). MSs may pose limitations on the right to access, in order to "(a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national

security; (e) protect the rights and freedoms of others". To this effect restrictions should be legally provisioned and follow the principles of necessity and proportionality.

Recommendation

Respond effectively and promptly to data subjects' requests exercising the right to access.

Similarly, data subjects should be awarded the right to rectification of his/her/their personal data, for instance, whenever data is inaccurate or incomplete, as well as the right to the erasure of personal data when processing is no longer necessary or is deemed unlawful.

Article 17 LED

As mentioned above competent authorities may, when necessary, proportionate and justifiable, limit the rights and information awarded to data subjects. In this line, the answers awarded to a data subject exercising his/her/their rights may vary from extremely detailed and comprehensive to mere neutral statements (please refer to annex II). Contextually, challenging such responses before a court is extremely challenging, especially considering it becomes difficult to define the object of the complaint (Sajfert & Quintel, 2017). As such, LED institutes Article 17, which provisions an independent review by the Supervisory Authority and allows for the indirect exercise of data subjects' rights.

Through this, LED effectively establishes a two-level system whereby (1) competent authorities are obliged to directly respond to data subjects' requests, providing them with the required information, to the extent possible, and (2) data subjects may indirectly exercise their rights by resorting to National Supervisory Authorities.

In this latter level, the Supervisory Authority must assess the lawfulness of processing, accuracy and completeness of personal data, subsequently rectifying and deleting it when necessary and justified. **Replies from Supervisory Authorities should, thus, be meticulously drafted to include information on this assessment, without revealing the grounds justifying the limitations imposed on the data subject's rights**. If the Supervisory Authority deems that the limitation is justified, its response should merely provide confirmation on the conduction of necessary assessment procedures and inform data subjects of the right to seek judicial remedy. This aligns with ECtHR jurisprudence, namely judgments *Roman Zakharov v. Russia* and *Szabò and Vissy v. Hungary* wherefrom one may infer the necessity to establish independent oversight of the lawfulness of processing, especially when data subject rights are restricted.

Recommendation

Replies from Supervisory Authorities should be meticulously drafted to include information on the assessment procedures conducted, without revealing the grounds justifying the limitations imposed on the data subject's rights.

Recommendation

Competent authorities should ensure data is processed in a secure manner, including by establishing procedures that prevent unauthorised access or use of personal data.

Security and Confidentiality

When determining the level of security, one should consider the state of the art, costs for implementation, the characteristics and purposes of the processing, and the risk posed to the rights and freedoms of data subjects. In this, **secure channels of communication between competent authorities and other involved entities should be ensured**. In case of a data breach, the competent authority should notify the supervisory authority without undue delay and, where feasible, no later than 72 hours after having become aware of it.

Transparency

As per Recital 26 LED, **data subjects should be cognisant of risks, rules, safeguards, and rights related to processing and they should be informed on how to exercise their rights.** Information should be easily accessible and drafted in a clear and comprehensive manner. **Competent authorities should disclose (1) purpose of processing, (2) identity of the data controller, (3) rights made available to the data subject, and (4) other relevant information required to ensure fair processing.**

Exceptions to the right of information are permitted, nonetheless, they should be provisioned in a legislative measure and respect principles of necessity and proportionality, and without prejudice to the right of data subjects to lodge a complaint and seek legal remedy (see annex II). **Restrictions to the right of information should be temporary, pre-determined and "framed by similar conditions, safeguards and limitations to those required under the Charter and the ECHR, as interpreted in the case-law of the CJEU and by the ECtHR respectively, and in particular respect the essence of those rights and freedoms"** (EDPB, 2021).

Recommendation

Competent authorities should be able to demonstrate that processing is performed in accordance with LED.

3. Obligations of the Controller under LED (see annex III)

In line with article 19, competent authorities should "implement appropriate technical and organisational measures to ensure and to be able to **demonstrate that processing is performed in accordance with [LED]**". Contextually, as per Article 6 LED competent authorities should **clearly differentiate personal data in accordance with categories of data subjects (*i.e.*, suspects, convicts, victims, witnesses)**. Law enforcement entities should thus **neatly tag and properly organise their databases**, in line with the jurisprudence of the ECtHR (See ECtHR case *Marper v. United Kingdom*, of 4 December 2008). Irrespectively, it bears noting that as Advocate General Sànchez-Bordona highlights, the inclusion of the provision "where applicable and as far as possible" within Article 6 LED provides some leeway to competent authorities. In fact, in situations where it might be hard to clearly determine if a data subject is a victim or a suspect, for instance when the situation develops during the pre-trial proceedings, it might not be possible to clearly distinguish these categories (Sànchez-Bordona, 2022; para 62 and ff).

Article 7 LED requires the establishment of a **distinction between personal data based on facts from that based on personal assessment.**

Recommendation

Competent authorities should clearly differentiate personal data in accordance with categories of data subjects as well as neatly tag and properly organise their databases.

Similarly, processing entities should strive to **integrate appropriate technical and organisational measures designed to safeguard by default data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing**. This should extend to the amount of personal data collected, the extent of the processing, period for storage and accessibility. (Article 20 LED).

Recommendation

Competent authorities should implement mechanisms of data protection by design and by default, such as integrating appropriate measures designed to, by default, safeguard data protection principles and integrate the necessary safeguards into the processing.

In accordance with Article 24 LED, competent authorities "should maintain a record of all categories of processing activities under their responsibility", therein including information in writing (including electronic format) on:

- name and contact details of the controller, joint controller and/or processor;
- purposes of processing;
- categories of recipients;
- description of the categories of the data subject and of the categories of personal data;
- if applicable, profiling;
- categories of transfers of personal data to a third country or an international organisation;
- legal basis;
- envisaged time limits; and
- general description of the technical and organisational security measures.

In this context, LED provides for the **obligation for competent authorities to keep logs of six processing operations in automated processing systems** (Article 25 LED). Therein, the Directive awards particular importance to the operations of consultation and disclosure as these are the most common and riskiest processing activities in databases. **These logs should** (Recital 57 LED):

1. identify the person who consults the database or who discloses the information;
2. identify the recipients of personal data.
3. disclose the exact date and time of the consultation or disclosure; and
4. inform on the justification for performing a processing operation;

As suggested by Sajfert and Quintel, **log collectors and monitoring procedures, such as random checks and pre-defined automatic alerts, may be implemented to identify irregularities and the misuse of data**. Monitoring can both be integrated manually or automatically. Logs can prevent grave data breaches, and should, in principle, **be kept for 2 years** (Sajfert & Quintel, 2017).

Recommendation

When resorting to automated processing systems, competent authorities should keep logs processing operations, by deploying log collectors and monitoring procedures.

Finally, on the topic of international transfer of personal data to third countries or international organisations, the **competent authority should certify the transfer satisfies the criteria laid in Chapter V of LED.** Generally speaking, the transfer should be based on an adequate decision and follow the principles provisioned under Article 35 LED, most importantly:

- transfer is necessary 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; and
- international data transfers may only be conducted through official channels, *i.e.*, between competent authorities.

In this, LED provisions a three-step system for international transfer. Firstly, the existence of an **Adequacy Decision** should ensure that the level of data protection in the third country is "essentially equivalent to that ensured within the Union" (CJEU C-362/14, Maximilian Schrems). Secondly, in the absence of said decision, the transfer should be subjected to **appropriate safeguards**, under Article 37 LED. Herein, either an appropriate safeguard shall be ensured through a legally binding and enforceable instrument (*e.g.,* EU-US Umbrella Agreement) or transfer should be based on a self-assessment evaluation carried out by the competent authority. Finally, Article 38 LED, allows for **derogation** from the conditions of Articles 36 and 37 thereof, in certain situations.

Recommendation

When conducting international transfers of data, it is important to certify the existence of an adequate decision for international transfers of data.

The Case for Asymmetric Transfers

In specific cases, the entity to whom data is transferred may be a private entity in a third country, for instance, an NGO. Such a transfer may be allowed in individual and specific cases, insofar as (Recital 73 & Article 39 LED):

- Transfer is necessary and proportionate;
- Public interest overrides the interest in the protection of the rights of the data subject (based on a decision of the competent authority for instance in the case of a threat to that person's safety or so as to prevent a terrorist attack);

- Transfering personal data to the competent authority in a third country is deemed not to be effective or appropriate for the specific purpose of processing, nor would it be possible to conduct it in a timely manner;
- The competent authority in the third country is informed without undue delay, save if deemed not to be effective or appropriate for the specific purpose of processing;
- The recipient is informed of the specific purpose or purposes for the processing of transferred data.

This mechanism surfaced with the primary aim of addressing cybercrime, especially considering its intrinsic characteristics and the need to directly cooperate with big enterprises, such as Google, Meta or Microsoft (Pejić, 2019; see also Sajfert & Quintel, 2017).

4. LED in the context of MIRAD and necessary relation to GDPR

In line with the Special Committee's report and the Counter-Terrorism Agenda for the EU, and the push for a multidisciplinary approach involving governmental bodies from all levels regardless of mandates and political agendas, non-governmental organisations, CSOs and NGOs, prison and probation staff, and the educational sector, the MIRAD project was envisioned to promote meaningful cooperation between governmental bodies and trustworthy community organisations, through holistic disengagement and reintegration programmes.

In this line, considering the above exposé, and following the apparent expansive definition of "public security", as adopted by the European Commission (COM(2022) 364 final), it becomes apparent that personal data processed in the context of the concerted action between competent authorities and CSOs and NGOs should follow a logic of implementation ***lex specialis* versus *lex generalis*** in reference to LED and GDPR respectively (Article 9 LED). Consequently, whenever data is processed by competent authorities, as defined above, for the purposes identified under Article 1(1) LED (in what concerns MIRAD the prevention of terrorist acts) LED shall apply. Subsequently, if processing exits the remit of this strict scope of application, for instance, if data protection is transferred to NGOs and CSOs, including subsequent processing, GDPR shall apply. In this context, legal basis for processing will follow that of Article 6(1)(e), (*i.e.*, performance of a task carried out in the public interest). This is because NGO and CSO action would not be governed under LED, insofar as they do not fulfil the personal scope of the Directive.

Following, it bears mentioning that data processing under GDPR is more restrictive, therein providing more safeguards to the data subject. As such, when data is transferred to a third party not covered by LED**, it is important for competent authorities to ensure that that third party is fully compliant with GDPR.** This could be achieved by assessing the respective entity's privacy policy and/or Data Protection Impact Assessment, if applicable.

Furthermore, when considering the activity of secret and intelligence services, it bears noting that their action has been widely integrated within "national security" (Bigo et al., 2014) and thus excluded from the scope of application of LED. Contextually, **data processing by these services should be governed by national law, in respect of Article 8 of the Charter and in line with the Council of Europe's Convention 108+.** This would also be applicable in the case that terrorism prevention is deemed to be a matter of national security, as opposed to public security, within national law. Irrespectively, one may infer that national provisions on data protection will not differ greatly from those under GDPR and LED, especially

considering the transposition exercise attached to EU Law. To this effect, without prejudice to potentially deviating from national law, most of the recommendations herein are transferable.

5. Differences between GDPR and LED

Provision	GDPR	LED
Transparency	Processing must be conducted in a transparent manner i.e., controller must take all appropriate measures to ensure that data subjects are informed about how their personal data is being used.	May be limited when proportionate, necessary and justified.
Data Minimisation	Processing of personal data must be limited to the extent necessary to fulfil a legitimate purpose, it should only take place when the identified purpose cannot be reasonably fulfilled through other means and it should not disproportionately interfere with the interests, rights and freedoms of the data subject.	The obligation to minimise the quantity of gathered personal data is weaker.
Rights of the data subject	The rights of data subjects may only be limited if necessary, proportionate and justified, to protect the rights and freedoms of others, or for a legitimate objective of general interest.	The rights of data subjects may be significantly restricted.
Consent	Under Article 6(1)(a) GDPR of the data subject is the legal basis by excellence.	Consent is not required as a legal ground for processing personal data by competent authorities.
Obligation to categorise data subjects	n/a.	Article 6 LED.
Requirement to distinguish personal data based on fact from that based on personal opinion	n/a.	Article 7 LED.
Obligation to keep logs of processing activities	n/a.	Obligation applicable to processing operations through automated means - Article 25 LED.
Obligation to provide time limits for the storage of personal data	Time limits should be established by the controller for erasure or for a periodic review	Time limits nationally provisioned – Article 5 LED
Data Transfers to Third Countries	Personal data may be transferred on the basis of an adequacy decision; appropriate safeguards; binding corporate rules; international	Personal data may be transferred to competent authorities on the basis of an adequacy decision;

	agreements (e.g., passenger name records); or derogations for specific situations.	appropriate safeguards; or derogations for specific situations. Additionally, it may be transferred to private entities under the mechanism of asymmetric transfers of Article 39 LED

Table 2 – Key differences between GDPR and LED

6. Practical Outlook from Field Experience

In the context of the MIRAD project, a preliminary iteration of the present Recommendation Paper was formally presented to a cohort of practitioners during an International Policy Roundtable[1] (IPR). The primary objective was to facilitate substantive deliberation amongst professionals, with the aim of identifying key obstacles and potential solutions pertaining to the application of LED, derived from empirical field experiences. The IPR participants' profile included policymakers, prison and probation staff, NGO/CSO representatives, and others from Poland, Belgium, Spain, France and Greece and other stakeholders from multilateral institutions such as the Radicalisation Awareness Network.

In order to facilitate this participative, co-creative process, IPR participants were challenged with the following four questions:

- What are the main challenges you can identify in complying with LED while ensuring effective information sharing and collaboration among agencies?
- How can inter-agency cooperation be enhanced to ensure efficient sharing of information while still upholding privacy rights and data protection principles?
- How do LED-related challenges impact the effectiveness of information sharing and collaboration among agencies while respecting individual privacy rights?
- Based on the recommendation paper, what additional measures or safeguards would you propose to enhance data protection in law enforcement practices?

Considering the answers garnered, these results may be condensed into two overarching sections.

What are the main challenges you can identify in complying with LED while ensuring effective information sharing and collaboration among agencies?

Compliance with LED while simultaneously ensuring efficient interagency information sharing and collaboration, presents several prominent challenges within the operational landscape. These challenges encompass various dimensions, reflecting the complexities inherent in striking a balance between data protection requirements and security. The primary difficulties encountered in this context, as identified include:

1. **Lack of Training and Education**: Inadequate training and education among law enforcement personnel regarding data protection provisions and best practices can impede compliance efforts and undermine the efficacy of information-sharing mechanisms;

[1] The IPR took place on the 28th of June 2023 in Brussels, Belgium. Further information concerning the aforementioned event can be found in D5.7 "International Policy Roundtable implementation report".

2. **Limited Access to Data Resulting in Compromised Risk Assessments**: Restricted access to pertinent data can impair the ability of competent authorities to conduct thorough risk assessments, potentially leading to suboptimal outcomes;
3. **Constraints Imposed by Storage Periods**: Mandated limitations on data retention periods, intended to safeguard privacy rights, may hinder the completion of essential investigative tasks within prescribed timeframes;
4. **Inter-Agency Data Exchange between Competent and Non-Competent Authorities**: The exchange of data between law enforcement agencies and non-competent authorities, such as social workers and non-governmental organisations (NGOs), results in ethical considerations and challenges relating to professional secrecy and to ensuring an appropriate flow of information;
5. **Balancing Societal Security and Data Protection**: Considering data protection is not an absolute fundamental right, striking an equilibrium between security and data protection principles poses significant challenges for competent authorities, as the pursuit of one may seemingly conflict with the other;
6. **Access and Hierarchy Considerations**: Issues concerning data access and the establishment of hierarchical levels of security clearance, both within and across agencies, introduce complexities in information sharing and collaboration, potentially impeding the timely and effective response to data subject request, and making it challenging to monitor unauthorised access;
7. **Overemphasis on GDPR Rendering LED to Oblivion**: The prevailing emphasis on the GDPR may have inadvertently overshadowed LED potentially leading to unintended non-compliance or oversight;
8. **Digitalisation and Electronic Evidence Challenges**: The increasing introduction of digitalisation and electronic evidence presents unique challenges in terms of ensuring the security, integrity, and admissibility of such data within the legal framework, while concurrently adhering to data protection standards;
9. **Security and Confidentiality in Inter-Agency Communications**: Inadequate communication channels among law enforcement entities, coupled with concerns regarding security and confidentiality, can impede the seamless sharing of data and hinder collaborative efforts.

How can inter-agency cooperation be enhanced to ensure efficient sharing of information while still upholding privacy rights and data protection principles?

To enhance inter-agency cooperation while upholding privacy rights and data protection principles, several strategies were identified. The following strategies were indicated as facilitating efficient sharing of information while adhering to stringent data protection standards:

1. **Creation of a List of Specific Personal Data**: Establishing a comprehensive list of specific personal data that can be collected, strictly defined and compliant with applicable data protection provisions, ensures a clear understanding of permissible information exchange. This list should

outline the types of data that can be shared among agencies, thus promoting clarity and consistency in data handling practices;

2. **Creation of a List to Identify Competent Authorities**: Especially considering the lack of clarity on the concept of "competent authority" as abovementioned, developing a list of competent authorities streamlines information-sharing processes;
3. **Creation of Models for Standardised Data Collection**: Establishing standardised models and protocols for data collection at various levels promotes consistency and compatibility. These models should encompass uniform data collection methodologies, ensuring that information can be seamlessly shared and understood across agencies while maintaining compliance with data protection principles;
4. **Set-Up Efficient Feedback Systems for Professionals**: Implementing efficient feedback mechanisms facilitates full compliance with data protection provisions. By establishing channels where professionals can communicate, share insights, and report feedback on data-sharing processes, agencies can refine their practices and align them with privacy rights and data protection principles. This promotes continuous improvement while maintaining a balance between information sharing, security and privacy;
5. **Resorting to Anonymity**: Implementing anonymisation techniques whenever possible and appropriate, can help protect individuals' privacy. In anonymising data, agencies are still able to extract valuable insights without compromising individuals' rights;
6. **Establishment of Ethical and Handling Codes**: Developing comprehensive ethical guidelines and handling codes specific to inter-agency data sharing ensures that all participating entities adhere to a shared set of principles. These codes should emphasise the responsible and secure handling of personal data, reinforcing the importance of privacy protection throughout the information-sharing process;
7. **Possibility to Request Judicial Orders**: Resorting to judicial orders or warrants to access personal data can provide strong legal safeguards. This ensures that access to sensitive information is granted only when justified and necessary for legitimate law enforcement purposes, thereby striking a balance between information sharing and privacy protection. Notwithstanding, some participants were quick to note that this may result in added time constraints that hinder the investigation and prevention of terrorism;
8. **Creation of Trust and Multi-Agency Systems**: Building trust among agencies through collaborative initiatives, joint training programs, and information-sharing agreements fosters a culture of cooperation while upholding privacy and data protection.

Conclusions and Recommendations

Summary

From the above exposé, it becomes clear that, at the EU and national level, a lot needs to be done in order to curb emerging doubts related to the scope of application of EU law, and competences awarded to the Union. Irrespectively, the overarching concerns over the protection of personal data in recent years, provide significant guidance on how to best protect data subjects' rights and balance them with the legitimate public interests. Following, and even if the still to be fully clarified by the Union, the topic of prevention of terrorism seems to fall under the overarching term "public security" and thus within the scope of LED, especially considering the expansive interpretation tendencies of the EU. In this line, it is important to safeguard the fundamental rights to privacy of suspects, victims, witnesses, convicted

persons, and other implicated parties, in light of the relevant Directive and Regulation. Based on LED, and GDPR as *lex generalis*, a number of different actions can be adopted, at the national and regional level, to ensure full data protection compliance. The following represent identified best practices and measures that can be adopted to that effect.

Recommendations

Recommendations for Policy Makers

1. MSs should maintain a list of entities considered "competent authorities" for the purposes of LED;
2. National Law should clearly define data protection and LED-specific terminology. Herein, concepts such as criminal offence, public security, national security, competent authority, should be the subject of comprehensive clarification that follows European law and jurisprudence;
3. MSs should clearly define the types of activities included under the umbrella of national security, thus delineating the actions covered under article 4(2) of the Treaty of the European Union, which are in turn excluded from the scope of LED;
4. Policy makers should establish models and protocols for standardised data collection, encompassing uniform data collection methodologies;
5. The purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguards against and the prevention of threats to public security should be provisioned within national law.

Recommendations for Competent Authorities under LED

1. Create a list of specific personal data to be collected;
2. Data processing should start with a comparison between the processing activity and the scope of application of LED so as to assess if it is covered by the provisions thereof;
3. Personal data must be obtained and processed lawfully and fairly;
4. Processing activities should clearly identify a specific, unequivocal purpose;
5. Processed personal data should not be excessive and should be adequate and relevant. It should not be kept for more than what is deemed necessary for the purposes for which it is being processed. In this, competent authorities should put in place appropriate mechanisms for the erasure of personal data, for instance by establishing periodic reviews of the necessity for storage of personal data;
6. Competent authorities should implement mechanisms, such as mutually agreed handling codes, a notification obligations or other transparency measures, to keep track of processing conducted by other entities;
7. Competent authorities should implement mechanisms of data protection by design and by default, such as integrating appropriate measures designed to, by default, safeguard data protection principles and integrate the necessary safeguards into the processing;
8. Personal data should be maintained in an accurate and up-to-date manner, without prejudice to the necessary considerations of the nature and purpose of processing;
9. Safeguards should be implemented to ensure that inaccurate data is not transmitted or made available and facilitate subsequent deletion or correction. Mechanisms such as classification systems of data (e.g., 4x4 grids for reliability assessments) and handling codes are good options;
10. Respond effectively and promptly to data subjects' requests exercising the right to access (see annex I and annex II);

11. Competent authorities should ensure data is processed in a secure manner, including by establishing procedures that prevent unauthorised access or use of personal data (use of secure channels of communication between competent authorities and other involved entities);
12. Competent authorities resort to anonymity when possible and necessary;
13. Competent authorities should clearly differentiate personal data in accordance with categories of data subjects as well as neatly tag and properly organise their databases;
14. Competent authorities should be able to demonstrate that processing is performed in accordance with LED;
15. Replies from Supervisory Authorities should be meticulously drafted to include information on assessment procedures conducted, without revealing the grounds justifying the limitations imposed on the data subject's rights;
16. When resorting to automated processing systems, competent authorities should keep logs processing operations, by deploying log collectors and monitoring procedures (e.g., random checks and pre-defined automatic alerts) to identify irregularities and the misuse of data;
17. When conducting a national transfer of data to entities not covered by LED, it is important for competent authorities to ensure that that third party is fully compliant with GDPR;
18. When conducting international transfers of data, it is important to certify the existence of an adequate decision for international transfers of data;
19. Competent authorities should set-up efficient feedback systems for professionals, by establishing channels where professionals can communicate, share insights, and report feedback on data-sharing processes,;
20. Implement trust and multi-agency systems through collaborative initiatives, joint training programs, and information-sharing agreements.

References

Legislation

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, OJ L 336, 10.12.2016, p. 3–13. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:22016A1210(01)

Charter of Fundamental Rights of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT

Council of Europe, European Convention on Human Rights. Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf

Council of Europe, Convention for the protection of individuals with regard to the processing of personal data. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon. OJ C 115, 9.5.2008, p. 345–345.

Directive (EU) 2016/680 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 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. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504

Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1686735515559

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol). Ammended and restated by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0794-20220628

Treaty on European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT

Treaty on the Functioning of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Jurisprudence

Court of Justice of the European Union (2020). Judgment of 16 July 2020, C-311/18, in the Case of Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

Court of justice of the European Union (2015) Judgment of 6 October 2015, in the Case , C-362/14 Maximillian Schrems v Data Protection Commissioner. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362

Court of Justice of the European Union (2017) Judgement of 20 December 2017, in the Case C-434/16, Peter Nowak v. Data Protection Commissioner. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0434

Court of Justice of the European Union (2021). Judgement of 8 December 2022, in the Case C-180/21, *REQUEST for a preliminary ruling under Article 267 TFEU from the Administrativen sad – Blagoevgrad (Administrative Court, Blagoevgrad, Bulgaria), made by decision of 19 March 2021, received at the Court on 23 March 2021, in the proceedings VS v.Inspektor v Inspektorata kam Visshia sadeben savet.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0180

European Court of Human Rights (1976). Judgement of 8 June 1976, in the case of Engel and others v. The Netherlands (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72). Retrieved from https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57479%22]}

European Court of Human Rights (2008) Judgement of 4 December 2008, in the case Case of S. and Marper v. The United Kingdom (Applications nos. 30562/04 and 30566/04). Retrieved from https://rm.coe.int/168067d216

European Court of Human Rights (2015). Judgement of 11 December 2015, in the case of *Roman Zakharov v. Russia* (Application no. 47143/06). Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}

European Court of Human Rights (2016). Judgement of 12 January 2016, in the case of *Szabò and Vissy v. Hungary* (App no 37138/14). Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}

Campos Sánchez-Bordona M. (2022). Advocate General Opinion of 19 May 2022 on the CJEU case C-180/21, VS v. Inspektor v Inspektorata kam Visshia sadeben savet. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62021CC0180

Reports and Publications

Abrunhosa, C., Liberado, P., & Djouadi, C. (2020). *Tailor-made exit programmes: different approaches for different social and political realities*. Wayout Project.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2007). *Opinion 4/2007 on the concept of personal data* | 01248/07/EN WP 136. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2014). *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges, Study for the Libe Committee, European Parliament Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs*.

Bozeman B., & Bretschneider S. (1994). *The 'Publicness Puzzle' in Organization Theory: A Test of Alternative Explanations of Differences between Public and Private Organizations*. 2 Journal of Public Administration Research and Theory 197.

Brewczyäñska, M. (2002). *Chapter 4: A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation*. In *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing. Retrieved from https://doi.org/10.4337/9781800371682.00013

Caruana M. (2019). *The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement*. 33(3) Int Rev Law Comput Tech 249, 252.

Council of Europe (2016). *Guidelines for prison and probation services regarding radicalisation and violent extremism*. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f5b69

Council of the European Union (2016). *Position (EU) No 5/2016 of the Council at first reading with a view to the adoption of a Directive of the European Parliament and of the Council 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, and repealing Council Framework Decision 2008/977/JHA*. OJ C 158 3.5.2016

European Commission (2022). *Communication from the Commission to the European Parliament and the Council First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED')*. COM/2022/364 final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0364

European Commission (2020). *Communication from the Commission to the parliament, the European Council, the Council of the European, the European Economic and Social Committee and the Committee of the Regionsa - Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795&from=EN

European Data Protection Board (2021). *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive.* Retrieved from https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012021-adequacy-referential-under-law_en

European Parliament (2018). *European Parliament resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism (2018/2044(INI)*. Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2018-0512_EN.html

EUROPOL (2022). *European Union Terrorism Situation and Trend Report (TE-SAT).* Retrieved from https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sa

EUROPOL (2023). *European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg*. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2023-te-sat#downloads

Marquenie, T. (2017).*The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework.* Computer Law & Security Review, 33, 324-340.

Martins, B., & Ziegler, M. (2018) *Counter-radicalisation as counter-terrorism: The European Union case*. In K. Steiner & A. Önnerfors (Eds.), *Expressions of Radicalisation* (pp. 321-352). Cham: Palgrave MacMillan.

Neumann, P. (2010). *Prisons and Terrorism: Radicalisation and Deradicalisation in 15 countries*. London: International Centre for the Study of Radicalisation and Political Violence [ICSR].

Pejić J. (2019) What is the EU Law Enforcement Directive? : How Law Enforcement Authorities (Should) Protect Personal Data[translation Ivan Kovanović]. Belgrade: Belgrade Centre for Security Policy. Retrieved from https://bezbednost.org/wp-content/uploads/2019/11/STA-JE-POLICIJSKA-DIREKTIVA-EVROPSKE-UNIJE-ENG.pdf

Purtova N. (2018). *Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships*. 8(1) Int. Data Priv. Law 52, 62.

Radicalisation Awareness Network (2016). *Approaches to countering radicalisation and dealing with violent extremist and terrorist offenders in prisons and probation*. https://home-affairs.ec.europa.eu/system/files/2019-07/ran_wrk_pp_pract_3rd-2018_20190606_en.pdf

Radicalisation Awareness Network. (2019). *RAN Collection of Approaches and Practices, Preventing Radicalisation to Terrorism and Violent Extremism*. https://home-affairs.ec.europa.eu/system/files/2021-05/ran_collection-approaches_and_practices_en.pdf

Sajfert, J., & Quintel, T. (2017). *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*. 2017. Retrieved from https://ssrn.com/abstract=3285873 or http://dx.doi.org/10.2139/ssrn.3285873

Vogiatzoglou, P., & Fantin, S. (2019). *National and public security within and beyond the Police Directive*. 2019. In Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), *Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*. Cambridge, Antwerp, Chicago: Intersentia, pp. 27-62

Welsh B., & Farrington D. (2012). *Crime Prevention and Public Policy*. In D. Farrington & B. Welsh (Eds) The Oxford Handbook of Crime Prevention.

Annexes

Annex I – Flowchart on right to access.

<table>
<tr><td rowspan="10">Assess and interpret request</td><td colspan="3">Does the request concern Personal Data?</td></tr>
<tr><td colspan="2">Yes – move to next step</td><td>No – No access granted</td></tr>
<tr><td colspan="3">Is the request based on Article 14 LED?</td></tr>
<tr><td colspan="2">Yes – move to next step</td><td>No – No access granted</td></tr>
<tr><td colspan="3">Does the request relate to the requesting person?</td></tr>
<tr><td rowspan="3" colspan="2">Yes – move to next step</td><td colspan="2">No</td></tr>
<tr><td colspan="2">Authorisation check</td></tr>
<tr><td>Yes – move to next step</td><td>No – No access granted</td></tr>
<tr><td colspan="3">Identity check</td></tr>
<tr><td colspan="2">Yes – move to next step</td><td>No – No access granted</td></tr>
<tr><td colspan="3">Assess the scope of the request and ask for specification if needed</td></tr>
<tr><td>How to answer the request</td><td colspan="3">• The competent authority should provide information on:
○ Whether or not personal data are being processed;
○ Access to data;
○ Additional information as identified in article 14 (a-g) LED.
• Information should be concise, transparent, intelligible, easily accessible and competent authorities should facilitate the exercise of the right of access facilitate the exercise of the right of access:
○ Choose the appropriate means – general rule information shall be provided in the same form as the request;
○ Provide a copy, if not agreed otherwise;
○ Use a layered approach if appropriate;
○ Timing – provide follow up to request without undue delay;
○ Free of charge.
• In order to retrieve data about the data subject, the competent authority should:
○ Define search criteria on the basis of the request;
○ Make use of technical functions available;
○ Search through all relevant filling systems (IT and non-IT);
○ Compile, extract or otherwise collect data that relates to the data subject in a way that fully mirrors the processing.</td></tr>
<tr><td rowspan="5">Limits and restrictions</td><td colspan="3">Are there legally provisioned limitations to the right of access or would rights or freedoms of others be affected by answering the access request</td></tr>
<tr><td colspan="2">Yes – No full access granted, act in accordance with limitation</td><td>No – Provide information to the data subject</td></tr>
<tr><td colspan="3">Is the request manifestly unfounded?</td></tr>
<tr><td colspan="2">Yes – charge a reasonable fee or refuse access</td><td>No – Move to next step</td></tr>
<tr><td colspan="3">Is the request excessive?</td></tr>
</table>

	Yes – charge a reasonable fee or refuse access	No – Move to next step
	Provide information to the data subject	

Table 3 - Flowchart on right to access

Annex II – How to respond to information requests.

Level 1	Competent authority decides to fully grant data subject rights.
Level 2	Competent authority decides to limit data subject rights in light of a legislative measure allowing for a limitation and provisioning a necessity and proportionality assessment for such limitations.
Level 3	Competent authorities decides not to provide any concrete information to the data subject opting instead for a neutral reply to his or her inquiry (Article 15(3) second sentence) – "we can neither confirm nor deny your data is being processed".

Table 4 - How to respond to information requests

Annex III - Data Protection Obligations

Obligations common to LED and GDPR	• Implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this directive (article 19); • Implement data protection by design and by default (article 20); • Use processors that provide sufficient guarantees and act only on instructions from the controller (article 22); • Maintain a record of processing activities (article 24); • Implement logging measures (article 25); • Cooperate with the supervisory authority in the performance of its tasks on request (article 26); • Carry out a data protection impact assessment when the processing is likely to result in a high risk to the rights and freedoms of natural persons (article 27); • Consult the supervisory authority in advance in the cases listed in article 28 of the directive; • Implement appropriate measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in article 10 (article 29); • Notify the supervisory authority of a personal data breach without undue delay, and, where feasible, not later than 72 hours after having become aware of it, when the breach is likely to result in a risk to the rights and freedoms of natural persons (article 30); • Communicate the personal data breach to the data subject without undue delay where the personal data breach is likely to result in a high risk to his/her rights and freedoms (article 31); • Designate a data protection officer under the conditions set out in article 32 of the directive;

	• Respect the conditions defined for the transfer of personal data to third countries or to international organisations (article 35 and following).
LED Specific Obligations	• Where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as persons convicted of a criminal offence, victims of a criminal offence, other parties to a criminal offence etc. (article 6); • Distinguish between personal data (personal data based on facts/personal data based on personal assessments) and ensure the quality of personal data (article 7); • Processing must be lawful (*i.e.*, Necessary for the performance of a task carried out by a competent authority) for the purposes of this directive, and based on union law or MS law (article 8); • Processing of special categories of data is allowed only where strictly necessary (article 10).

Table 5 - Data Protection Controller Obligations