# VI. The Role of Technology in Detecting and Preventing Crime, and Data Protection Issues

# New developments in data protection in the EU-US cooperation in criminal matters

ELS DE BUSSER
*Dr. jur., Senior Lecturer(European Criminal Law) and Senior Researcher (Cyber Security) at the Hague University of Applied Sciences*

2016 is a most interesting year for data protection in the EU.[1] At the end of 2015 signs were clear that the negotiations on the so-called data protection reform package were nearing their conclusion. In spring 2016 both legislative instruments – the Directive[2] on 5 May and the General Data Protection Regulation[3] on 24 May – finally entered into force starting the two year term for the Member States to implement the new rules. Parallel to these legislative processes the debates between EU and US officials were running concerning an EU-US Agreement on data protection for law enforcement purposes, also known as the Umbrella Agreement. The Umbrella Agreement was signed on 2 June 2016. On top of that the aftermath of the Schrems case before the

[1] This paper is an updated version of an article published as E. De Busser, 'The future of transatlantic data protection in criminal matters', Forschungsbericht Max Planck Institut für ausländisches und internationales Strafrecht, Freiburg, 2015.

[2] Regulation (EU) 2016/679 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, O.J. L 119, 4.5.2016, (further: General Data Protection Regulation).

[3] 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, and repealing Council Framework Decision 2008/977/JHA, O.J. L 119, 4.5.2016, (further: Directive on data protection in criminal matters).

Court of Justice[4] resulted in a new EU-US Privacy Shield.[5] Even though the latter concerns data protection in commercial matters, specific elements have repercussions on data protection in criminal matters. This contribution will first zoom in on the general data protection standards in criminal matters, their origin and their meaning before moving on to the latest developments in this field and the new legal instruments in the EU as well as in the EU-US cooperation as well as their after-effects.

**Data Protection Legal Framework**

In view of potential negative effects on the rights of individuals, the collecting and processing of personal data is restricted by national, European, and international legal instruments. The data protection rules applicable in the EU are based on principles laid down by the Council of Europe (CoE) in the 1981 Data Protection Convention.[6] The CoE introduced these data protection principles in response to shortcomings of the right to a private life (Article 8 European Convention on Human Rights (ECHR)) in the context of a growing use of information technology. This "mother convention" of data protection dictates the principles or standards that should minimally be respected when personal data are processed by automatic means, regardless of the type of data or the purpose they are processed for. EU legal acts and national laws on data protection are in turn based on these general rules. Above all, in 2009 the EU Charter of Fundamental Rights and Freedoms introduced an innovative right to protection of personal data alongside the right to a private life.[7]

The general data protection standards from the Data Protection

[4] C-362/14, Schrems v Data Protection Commissioner, 2015.

[5] Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176 final.

[6] 1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 (further: the Data Protection Convention).

[7] EU Charter of Fundamental Rights and Freedoms, *O.J.* C 364, 18.12.2000.

Convention are applicable when data are processed for commercial purposes with consent as the core requirement. An individual needs to give his or her explicit consent before data are collected and processed if not specifically regulated by law. In criminal matters, the general data protection standards are applicable provided additional conditions are in place. In the first place, these conditions safeguard fair trial rights such as the presumption of innocence. E.g. when personal data on a suspect are processed, it should be clear that these data concern a person who is suspected of a crime but not convicted. Secondly, the consent requirement that forms the basis of data protection in commercial matters, does not work in a criminal investigation. Gathering personal data for the purpose of a criminal investigation is mostly done without the individual's knowledge – e.g. tapping his or her telephone – and thus requires additional rules concerning the purpose of the processing and the competence of the authority that processes the data. In principle, general data protection standards are also applicable to gathering intelligence in so far as intelligence contains personal data and considering certain exceptions. Still, it is crucial to distinguish data processed and exchanged for intelligence purposes from those processed and exchanged for criminal investigations. While criminal investigations conducted by law enforcement authorities are based on the suspicion of a criminal offence and with the goal of using the data as evidence in criminal proceedings, intelligence activities are carried out without such suspicion and for the protection of national security. In the latter case, the data are in principle secret. Moreover, they can be based on unverifiable assumptions and conclusions making the accuracy and reliability of the data questionable. Besides the difference in purpose, national security is also an exclusive national competence. The EU legislator is unable to draft any provisions in this area. International agreements on the exchange of intelligence are rare, whereas the exchange of data for criminal investigations is frequently laid down in bi- or multilateral agreements. This makes data protection in the case

of intelligence a rather obscure area, only dealt with by the CoE in non-binding recommendations.[8]

Compliance with EU data protection rules is the responsibility of the data controllers, the (natural or legal) persons or authorities determining the purposes and means of processing. A data controller located outside the EU but using processing equipment and processing personal data on EU territory is bound by the EU data protection rules. This means that foreign companies engaging in commercial activities within the EU should process their customers' personal data in compliance with EU data protection legislation. When data are transferred for commercial purposes or for law enforcement purposes, a recipient state outside the EU – such as a US company – should have an adequate level of data protection. This is a challenging requirement to fulfil considering the differences between the EU's and the US' data protection system; it even raises the question whether, as a matter of principle, the EU should exchange personal data with the US. When considering possible models for exchanging data and bridging the gap between the two data protection frameworks it is necessary to examine how substantial the differences are and what the priorities in any solution model should be.

**European Principles**

The principles formulated in the CoE Data Protection Convention were further specified in order to regulate data processing in the EU. For the purpose of commercial activities this was done in Directive 95/46/EC[9] (the Data Protection Directive) and for law enforcement purposes in Framework Decision 2008/977/JHA[10] (Framework Decision on

[8] Recommendation regulating the use of personal data in the police sector, No. R(87)15, 17.9.1987.

[9] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L281, 23.11.1995.

[10] Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J.

data protection in criminal matters). They can be divided into principles safeguarding the quality of personal data on the one hand, and principles safeguarding the quality of processing of personal data on the other.

1. *Quality of personal data*

Personal data is any information that identifies or enables to identify an individual, e.g. a name, phone number or even an IP address.[11] Since personal data are not necessarily permanent, they shall be corrected when inaccurate as well as completed or updated when possible and necessary. This goes for commercial matters as well as for criminal matters, although in criminal matters the consequences for the individual involved can be more far-reaching when incorrect or unreliable data are processed. Therefore, when personal data are used for law enforcement purposes it is essential to indicate their degree of accuracy and reliability and to distinguish facts from assessments or opinions, e.g. data on the behaviour of a suspect. The CoE recommended[12] making such a distinction, but did not make this a binding principle even though it was endorsed explicitly in binding legal instruments, e.g. the Europol Decision. The new EU directive on data protection in criminal matters makes indicating the degree of accuracy and reliability of personal data an obligation for all law enforcement agencies.[13]

In both commercial and criminal matters, personal data should be adequate, relevant, and not excessive in relation to the purpose they are collected and processed for. Collecting data for a potential future use is forbidden. Respecting the proportionality rule means that the data controller should, for each case, determine and distinguish the minimum amount of personal data needed in order to successfully accomplish the purpose.

---

L 350, 30.12.2008.

[11] Article 29 Data Protection Working Party, Opinion 4/2007, 20.06.2007.

[12] Recommendation regulating the use of personal data in the police sector, No. R(87)15, 17.9.1987.

[13] Article 7, Directive on data protection in criminal matters.

2. *Quality of personal data processing*

The general principle is that personal data should be collected for a specific legitimate purpose and should not be processed for purposes that are incompatible therewith. The purpose limitation principle can be derogated from if this is laid down in law and only if the data are necessary in the interests of *inter alia* the suppression of criminal offences. E.g. when data are collected for commercial purposes by a company and processed by law enforcement agencies this would constitute an incompatible purpose. For this processing to be allowed, a nexus with a criminal investigation should be present, e.g. data on the purchase of a printer after investigation has revealed this printer was used for printing counterfeit euro notes. The background of these lawful derogations lies in the right to a private life as provided for by Article 8 ECHR. In accordance with the ECHR, any limitation to the right to a private life should be legal and necessary in the interests of a legitimate aim.

Even when personal data are adequate and relevant at the moment of their collection, it is not unimaginable that, after a certain amount of time, these data are no longer adequate and relevant in relation to the purpose they were gathered for. The data retention principle obliges the data controller to store personal data in databases for as long as is required for the purpose they are processed for. After this period of time has passed, the data can still be retained but need to be separated from the name – the identifying factor – of the individual they relate to. The data retention principle can also be derogated from under the same legality and necessity conditions as described above.

3. *Rights and remedies*

When individuals wish to act against unlawful processing of their personal data by a data controller, independent supervisory authorities have been set up on a national level to receive and treat complaints. If necessary, these data protection authorities can initiate legal proceedings. Besides the administrative remedies before supervisory authorities, judicial remedies are part of the data protection standards in

commercial matters as well as in criminal matters. Not only EU citizens can submit complaints for unlawful processing of personal data, as the data protection authorities are equally accessible to non-EU citizens as long as the data processing occurred on EU territory.

4. *Transferring personal data*

International cooperation in criminal matters implies exchange of personal data. Transferring personal data between the EU Member States does not – in principle – present any risks as all are bound by the same data protection standards. The risk of personal data being collected and processed unlawfully however exists when data are transferred to a third state. This can still be a state that has ratified the Data Protection Convention, or this can be a state that did not ratify and applies a completely different data protection system; the textbook example for the latter is the US. Nevertheless, EU-US cooperation, including the transfer of personal data, continues to take place. This is where the adequacy requirement comes in: before a transfer of personal data can take place, the recipient state's level of data protection should be assessed as adequate from an EU point of view. First introduced in Directive 95/46/EC the requirement was also incorporated in the Framework Decision on data protection in criminal matters and in the 2001 Additional Protocol to the CoE Data Protection Convention.[14] Adequate does not mean identical; it means that in view of all circumstances related to the specific data transfer the extent to which the data protection standards are met in the recipient state and the means by which the data subject can defend his or her interests in case of non-compliance should be acceptable. The adequacy requirement is applicable in commercial matters as well as in criminal matters. Derogations from the requirement are allowed when legitimate interests prevail or when adequate safeguards are offered.

As the adequacy requirement is a part of the EU and CoE data protection standards, it makes interstate cooperation dependent on the re-

[14] Additional Protocol, ETS No. 181.

cipient state fulfilling a condition that it did not endorse. Since the US did not ratify the Data Protection Convention, it should provide in an adequate level of data protection to receive personal data from an EU Member State or agency. A parallel can be drawn with extradition law, where the third state requesting an individual's extradition should give assurance that it will neither carry out the death penalty nor subject the individual to inhuman or degrading treatment or punishment before an extradition can take place. In the landmark Soering case before the European Court of Human Rights,[15] the US – not a party to the ECHR – nonetheless saw their request for extradition being outweighed by the human rights argument. In other words, a state's obligation to either extradite or prosecute is overruled by the prohibition of torture or inhuman or degrading treatment or punishment. Could one argue that in the case of the adequacy requirement a state's obligation to cooperate is overruled by the right to a private life and the protection of personal data? Not quite, since there is a substantial difference between the human rights involved: the prohibition of torture or inhuman or degrading treatment or punishment is known as an absolute right not allowing derogations, whereas the right to a private life allows for more restrictions and exceptions.[16] Therefore, cooperation involving personal data exchange can still be carried out with a third state that does not fully respect the data protection standards.

The adequacy requirement is unfortunately marred by some inconsistencies such as the lack of uniform application by comparable data controllers. Europol and Eurojust – both EU agencies processing personal data for the purpose of criminal investigations and prosecutions – have drawn up different procedures for reaching a decision on the adequacy of a third state's data protection level. While Europol – apart from urgent matters – applies a four-step filtering system for reaching such a decision, Eurojust relies on only one step by letting its data pro-

[15] ECtHR, Soering v United Kingdom, 7.7.1989.

[16] See elaborately: E. De Busser, 'Flagrant denial of data protection – redefining the adequacy requirement", *Transatlantic Data Privacy Relationships as a Challenge for Democracy*, European Integration and Democracy Series, Vol. 4, 2016, in print.

tection officer decide on the matter. For an area that is as sensitive as international cooperation in criminal matters dealing with personal data on suspects, victims, and witnesses, this difference in dealing with data transfers is considerable.

Inconsistencies regarding the adequacy requirement are intensified when examining the EU-US cooperation in criminal matters. Data exchange in accordance with the 2002 Europol-US Agreement was initiated without a full adequacy assessment but based on the urgency exception. This agreement organised the exchange of personal data held by Europol – thus also including data received from Member States police authorities – with the competent US authorities. Eurojust concluded a cooperation agreement with the US in 2006, including the exchange of personal data. The same formulation as included in the 2003 EU-US Mutual Legal Assistance Agreement was used, namely no "generic" restrictions for processing of data with respect to the legal standards of the receiving party may be imposed as a condition for delivering information. This is a rejection of the adequacy requirement. When personal data gathered for commercial purposes are transferred for law enforcement purposes, a similar trend is visible. The 2010 EU-US Agreement on the Processing and Transfer of Financial Messaging Data for the Purposes of the Terrorist Finance Tracking Programme introduced the concept of assumed adequacy by stating that the recipient US Treasury Department is deemed to ensure an adequate level of data protection for the purposes of the agreement.

Because the US data protection legal framework does not live up to the EU requirement of an adequate level of data protection, a compromise was found by setting up the so-called Safe Harbor agreement. This list of commitments based on the EU data protection standards was signed by a number of US companies enabling them to continue their business activities on EU territory and process personal data from EU citizens.[17] In 2000 the European Commission confirmed that the Safe Harbor agreement represented an adequate level of data protec-

[17] Decision 2000/520/EC, O.J. L 215/7, 25.8.2000.

tion. It was this Commission decision that was annulled on 6 October 2015 by the Court of Justice in the Schrems case.[18] This made the Commission start work on a new compromise replacing the Safe Harbor agreement. The result was the EU-US Privacy Shield, adopted on 12 July 2016.[19] The Privacy Shield is just like Safe Harbor based on self-certification by companies who commit themselves to comply with the data protection standards listed by the agreement. A significant part of the Privacy Shield is the assurance from the US that the access of public authorities for law enforcement and national security purposes is subject to clear limitations, safeguards and oversight mechanisms.

On 2 June 2016 another agreement was signed between the EU and the US, the Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses. Also known as the EU-US Umbrella Agreement, this legal instrument offers a general framework of data protection to the transatlantic data exchanges for law enforcement purposes. When presenting the draft agreement in February 2016, Commissioner for Justice, Consumers and Gender Equality Věra Jourová stressed that the text would not enter into force as long as the US Privacy Act redress mechanisms were not applicable to EU citizens. It had long been a point of discussion among privacy experts that the protection offered by the 1975 US Privacy Act[20] was restricted to US citizens and residents.[21] As a consequence, any non US citizen whose personal data are collected or processed unlawfully by US authorities could not submit a complaint based on the Privacy Act. Using this lack of redress as leverage, the Commission achieved indeed the signing of the US Judicial Redress Act by President Obama on 26 February 2016.[22] It should be highlighted that the US Judicial Redress may be an improvement to the situation for EU citizens, yet it does not mean there are no strings at-

[18] C-362/14, Schrems v Data Protection Commissioner, 6.10.2015.

[19] See fn. 5.

[20] 5 USC 552a.

[21] 5 USC § 552a(a)(2).

[22] Public Law No: 114-126, 2.24.2016.

tached. First of all, the Judicial Redress Act opens the Privacy Act's redress mechanism to citizens of „designated countries". Which countries are among the designated countries is for the Attorney General to list and make public in the Federal Register. Secondly, in spite of the US' criticism on the adequacy requirement applicable in Europe, the Judicial Redress Act introduces an American version of this condition. Thirdly, no matter how beneficial it is for EU citizens to have the opportunity to file a complaint against unlawful processing of their data, it will never be an effortless task to be aware of such processing by US authorities.

**US Data Protection Standards**

Based on the aforementioned adequacy requirement and the data protection standards of the EU, the US' data protection framework is briefly examined in the following part, taking into consideration the issues uncovered by former NSA contractor Edward Snowden in 2013. The US' data protection system is structured in a different manner compared to the EU's tradition of umbrella legislation and general principles. Even though the Snowden revelations dealt with intelligence that was primarily gathered by the NSA and not transferred by national authorities, the scandal highlighted two key elements of the transatlantic relationship that are also significant for the cooperation in criminal matters: the willingness and widespread practice of telecommunication companies to make data available to US authorities, and the lack of rights for non US persons. Finally, caution should be taken when comparing the concept of law enforcement as it is understood in the EU to the concept's meaning in the US.

The lack of an adequate level of data protection in the US will, in the following parts, be illustrated by using the context of the Snowden revelations – although this concerns intelligence and not data gathering for criminal investigations and prosecutions – on the one hand, and the EU-US negotiations on a possible transatlantic agreement on data exchange in criminal matters on the other.

1. *No general data protection standards*

Since the US' data protection framework does not consist of umbrella legislation, the purpose limitation and data retention principles do not have generally applicable US counterparts. They can be found in specific laws (e.g. Privacy Act and Children's Online Privacy Protection Act), sector specific laws or in industry self-regulation instruments. Nevertheless, exceptions to these rules should be studied carefully.

Illustrating the importance of exceptions in US legal provisions dealing with privacy and data protection, one of the American data quality standards can function as an example: accuracy of data is a requirement in the US Privacy Act. When an interagency transfer of data takes place however, law enforcement and intelligence agencies are exempted from this rule.[23] Furthermore, the Privacy Act contains a general exemption for data maintained by agencies that have criminal law enforcement as their principal function and process data for the purpose of identifying an offender, a criminal investigation, or any stage of the process from arrest to release from supervision.[24] This example demonstrates how far-reaching the exceptions to data protection rules of the Privacy Act can be.

2. *Lack of rights for EU citizens*

After the Judicial Redress Act made the Privacy Act applicable to non US citizens, lacking rights for EU citizens in US legislation is still visible in other provisions, such as provisions on foreign intelligence. The US Patriot Act of 2001,[25] amending and expanding the provisions of the Foreign Intelligence Surveillance Act of 1978, contains two sections that are designed to collect data on non-US persons: Section 215 on the gathering of telephone data[26] – numbers dialed and duration of

[23] 5 USC § 552a(e)(5) and (6).
[24] 5 USC § 552a(j)(1) and (2).
[25] Public Law 107–56, 26.10.2001. See 50 USC 1804(a)(7)(B) and 1823(a)(7)(B)).
[26] 50 U.S.C. 1861 *et seq*.

the call, not the content of communication– with the assistance of telecommunication providers, and Section 702 on obtaining data on non-US persons reasonably believed to be located outside the US.[27] Heavily criticized for its lack of necessity and proportionality, reports by the Privacy and Civil Liberties Oversight Board (PCLOB)[28] and the President's Review Group on Intelligence and Communications Technologies[29] published after the Snowden revelations, called for the end of Section 215. The section expired automatically on 1 June 2015, after which a transition period of six months was authorized. The impact of Section 215 on non-US persons is not analysed in the post-Snowden reports, even though the programme's objective is "to obtain foreign intelligence information not concerning a US person or to protect against international terrorism or clandestine intelligence activities". Remarkably, it was Section 702 that was not only considered a necessary programme but also triggered statements from US policymakers on the impact on non-US persons. The PCLOB even stated that if Section 702 was drafted to intercept communications of US persons, it would violate the Fourth Amendment.[30] The aforementioned Judicial Redress Act redeems this situation of lacking rights for non-US citizens.

3. *Law enforcement*

As mentioned in the introduction, collecting data for law enforcement purposes should, in the EU, be distinguished from collecting data for intelligence and security purposes. This tradition on separating law

[27] 50 U.S.C. 1881a.

[28] PCLOB Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23.01.2014.

[29] 'Report and recommendations of The President's Review Group on intelligence and communications technologies', 12.12.2013, 103, https://www. whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[30] *Ibid*., 153. See also United States v. Verdugo-Urquidez, 494 US 259, 265-266 (1990).

enforcement and intelligence purposes does not have an equivalent in the US system, although in principle, the divide was visible in the 1947 National Security Act. A legislative wall that was firmly in place in order not to use data gathered for intelligence purposes in criminal investigations was gradually dismantled, with the most significant steps taken in the 2001 Patriot Act.

That such difference in understanding a basic concept can lead to difficult transatlantic discussions was obvious from the 2008 reports of the High Level Contact Group.[31] Preparing a general EU-US agreement on data exchange in criminal matters, this group of EU-US senior officials aimed to draft common concepts, including law enforcement purposes. The report stated that in the EU, this covers the use of data for the prevention, detection, investigation, or prosecution of any criminal offense while in the US, it encompasses the "prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security as well as non-criminal judicial or administrative proceedings related directly to such offenses or violations".

It is clear that for the US the concept of law enforcement includes more than just police officers; it also includes national security and even migration officers. While developing an EU-US agreement on data exchange in criminal matters, it is remarkable that both parties are speaking of something completely different when using the same terminology. A solution to bridge this gap has not been offered yet.

**Concluding Remarks**

This contribution only scratched the surface of the wide theme that is data protection and technology in criminal matters. The delicate part of writing on a topic that is in full development is that the moment you finish a contribution it can be outdated already. Which is why certain parts of this contribution may no longer be valid soon. With this caveat

[31] Council, 9831/08, EU US Summit, 12.6.2008 – 'Final report by EU–US High Level Contact Group on information sharing and privacy and personal data protection', 28.5.2008, p. 4.

in mind it is relevant to shed light on these developments, some of which can easily be overlooked.

No one can deny that data protection and technology go hand in hand, be it in commercial matters or in criminal matters. In criminal matters however, an additional sensitivity arises due to the fundamental rights that are at stake such as the fair trial rights. Personal data being used in a criminal investigation or prosecution crossing the EU's external borders to be processed in another jurisdiction, opens up a whole range of other questions. This is certainly the case when that other jurisdiction is the US, due to its essentially different – from a European perspective – data protection legal framework but also due to the recent revelations on data gathering and processing by US authorities. The introduction of the long awaited EU-US Umbrella Agreement on data protection for law enforcement purposes and the US Judicial Redress Act improving redress opportunities for EU citizens in the US, should be welcomed. Nonetheless, we should be careful with applauding too soon.

The practicalities of first, being aware of unlawful data processing by US authorities and second, submitting a successful complaint under the terms of the Privacy Act, create a daunting task for any EU citizen unfamiliar with the US legal framework. This could lead to three particular after-effects: first of all, many data subjects who are aware of unlawful data processing by US authorities will not take legal action out of fear for lengthy and costly proceedings; second, of those who do take legal action, many will be discouraged by difficult and lengthy proceedings and satisfy themselves with settling the case out of court; and third, this could produce a new type of litigation lawyer who is specialized in EU data protection law as well as the US legal system, has in depth knowledge of the EU-US agreements in force and is admitted to the relevant US state bar.

Immediately after the main points of the text of the General Data Protection Regulation were public, consultancy firms started publishing guidelines for businesses who needed to adjust their data protection approach. A similar development – although on a smaller scale –

was visible after the EU-US Privacy Shield was presented. Both are legal instruments in commercial matters, involving an enormous amount of companies who could use some practical advise on how to deal in practice with the new provisions. We do not see a similar approach in the area of criminal matters. Apart from the excellent publications by the European Data Protection Supervisor, no guidelines have been issued on how a data subject should handle his or her personal data being unlawfully processed for the purpose of a criminal investigation or prosecution.

Considering that the fundamental rights and freedoms at stake in criminal cases are of essential value, it is surprising that the majority of attention is paid to the new instrument on data protection in commercial matters. Awareness, training and practical guidance are three points that are often taken for granted when new legal instruments are presented. In an area of law that is formed by the intersection of criminal law and data protection law and is thus susceptible to have a crucial impact on the life of a person, these points undoubtedly deserve more attention.