Article 25. Logging

Michael Veale, Faculty of Laws, University College London

To appear in:
The Law Enforcement Directive: A Commentary (Kosta & Boehm, eds., Oxford University Press 2023)

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.
2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.
3. The controller and the processor shall make the logs available to the supervisory authority on request.

Relevant Recitals

(56) In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(57) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing. Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

Closely Related Provisions

Article 4(1)(f) and 4(4) (principles relating to the processing of personal data, especially on security and accountability) (see also recital 28); Article 19 (obligations of the controller) (see also recital 50); Article 20 (data protection by design and by default) (see also recital 53); Article 24 (records of processing activities) (see also recital 56); Article 29 (security of processing) (see also recital 60); Article 30(5) (notification of a personal data breach to the supervisory authority, in particular relating to documentation requirements) (see also recital 61); Article 37(3) (transfers subject to appropriate safeguards, in particular relation to documentation) (see also recital 72); Article 47(1) (powers of the supervisory authority, in particular relating to information gathering) (see also recital 82); Article 63 (2–3) (transposition, in particular relating to logging) (see also recital 96).

Related Provisions in GDPR [Regulation (EU) 2016/679]

Article 5(1)(f) and 5(2) (principles relating to the processing of personal data, especially on security and accountability); Article 24 (responsibility of the controller); Article 25 (data protection by design and by default); Article 30 (records of processing activities); Article 32 (security of processing); Article 58 (powers of the supervisory authority).

Related Provisions in EUDPR [Regulation (EU) 2018/1725]

Article 88 (Logging) (see also recital 52); Articles 4(1)(f) and 4(2) (principles relating to the processing of personal data, especially on security and accountability); Article 26 (responsibility of the controller); Article 27 (data protection by design and by default); Article 31 (records of processing activities); Article 33 (security of processing); Article 48(5) (transfers subject to appropriate safeguards, in particularly relating to informing the European Data Protection Supervisor); Article 58 (powers [of the European Data Protection Supervisor]).

Relevant Case Law

CJEU

Case C-553/07, *Rijkeboer* (ECLI:EU:C:2009:293).

ECtHR

I v. Finland, Appl. No. 20511/03, judgment of 17 July 2008.

National cases

Judgment of the Raad van State of 25 November 2009, (ECLI:NL: RVS:2009:BK4335) (Netherlands).

A. Rationale and Policy Underpinnings

There are several overlapping logics for mandating logging. The LED states that logs should be used solely for the 'verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.'[1] This can be split three ways and the logics analysed further as follows.

1. Logging for Integrity and Security

Firstly, logging and the review of logs can be an important part of the computer security required by clause 4(1)(f) LED, often referred to as the 'security principle'. ISO/IEC 27002, an important global technical standard for information security management, requires that 'logs recording user activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed'.[2] Logging of system usage can help mitigate attacks through the use of real-time automated monitoring systems, and support retrospective investigation of incidents and subsequent system fortification.[3] For example, in the Netherlands, the LED's logging provisions in Article 25 LED are bring used to introduce real-time systems to monitor police use of data and detect misuse.[4] Relevant to this purpose of logging are the separate requirements in the LED for controllers to ensure the possibility to verify who and when data records were amended or added, or transferred; 'input control' and 'communication control' respectively.[5]

Logging itself entails security and integrity considerations. The CNIL recommends logging data be kept on a separate physical system where the system being logged has no possibility of overwriting logging data.[6]

2. Logging for Self-Monitoring and Verification of Lawfulness

[1] Art. 25(2) LED.
[2] ISO/IEC 27002:2022 section 8.15.
[3] CNIL 2021.
[4] Tweedekamer 2021.
[5] Art. 29(2)(f)-(g) LED.
[6] CNIL 2021.

A second logic of logging is in order to ensure accountability for compliance with the data protection regime.[7]

Logging can support *internal accountability*. For example, logging may support data minimisation efforts by evidencing the frequency of use of data and informing retention periods or collection scope. It may equally be used to evidence needs for broader or longer collection practices. Logging may further enable developers to alter user interfaces and system design to best meet legal data protection by design requirements.[8] For example, logging may reveal that large amounts of sensitive data are routinely disclosed to individuals who only need a specific fact or portion that could be provided independently. These roles may be undertaken by the data protection officer, whose roles include monitoring compliance with the LED.[9] Further to this, the recitals counsel that self-monitoring encompasses internal disciplinary proceedings within a competent authority.[10]

Logging further supports *external accountability*. This will typically be to DPAs, who may request logs to investigate suspected illegality.[11] There are a variety of ways logs themselves may be personal data, either to the workers accessing the processing systems, or potentially to those that operations specifically relate.[12] Rights of access, or other civil procedural rules in national courts, may result in such data being obtained for accountability purposes. Where data is unable to be provided to data subjects on legal grounds, DPAs may be involved as intermediaries in analysing logs on behalf of data subjects.[13]

Logging may also support *accountability across chains or data processing.* Contemporary data processing in the law enforcement domain may see data pass between national law enforcement authorities; to private bodies as processors, independent or joint controllers, and/or competent authorities delegated to by Member State law;[14] across borders both to competent authorities and to other bodies;[15] or to international

[7] Art. 4(4) LED.
[8] Art. 20 LED.
[9] Art. 34(b) LED.
[10] Rec. 57 LED.
[11] Art. 47(1) LED.
[12] CNIL 2021.
[13] Art. 17 LED.
[14] Art. 3(7)(b) LED.
[15] Art. 39 LED.

organisations.[16] Understanding these flows may be important to ensure legality of actions taken with those data in light of both national and European law.

3. Logging for Criminal Proceedings

The final logic behind logging is the newest in European law – its utility in criminal proceedings. In extreme situations of accountability, where data misuse may have constituted a criminal offence, logs may also be admissible in court. In the FD, logs could only be used in order to verify the legality of processing, self-monitoring and data security and integrity.[17] The LED extends this to allow logs to also be used in criminal proceedings,[18] but the scope of this ground remains unclear, and is further discussed below.[19]

B. Legal Background

1. EU legislation

EU law relating to cross-border information systems established under the former JHA pillar routinely required that certain actions relating to these systems should be logged. For example, the 1995 Customs Information System (CIS) Convention requires Member States to guarantee that "it is possible to check and establish a posteriori what data has been introduced into the [CIS], when and by whom, and to monitor interrogation".[20] The 2000 Convention Implementing the Schengen Agreement (CISA) similarly requires that 'transmission and receipt of personal data [communicated pursuant to this Convention] must be recorded both in the source data file and in the data file in which they are entered', and these logging obligations extend in certain situations even to non-automated data.[21] It therefore was unsurprising when, filling the gaps in these regimes, the FD introduced similar, albeit more generic, logging obligations.[22] These were limited to transfers, and solely for the purpose of verification of legality by supervisory authorities. This limitation was criticised at the time by the EDPS and the European Parliament, who both argued that *access* to personal data should be logged.[23]

[16] See generally Purtova 2018.
[17] Art. 10(1), FD.
[18] Council Position 2016.
[19] See below, section C.2.
[20] Art. 19 CIS Convention 1995.
[21] Arts. 126(3)(e) and 127(2)(a) CISA 2000.
[22] Art. 10 FD.
[23] EDPS 2007, p. 2; European Parliament 2008, amendment 13.

The provision in the LED remains mostly unchanged from the LED proposal, with a few important exceptions.[24] The final text of the LED clarifies that 'transfers' are included within the notion of 'disclosures.' The version in the LED narrows the scope of logging obligations to only automated processing, even though the LED applies to manual processing within a filing system.[25] It also more loosely describes the content of logs. In the LED proposal, logs had to *show* the information described; in the LED, they need only *make it possible to establish*, a construction which may allow more flexibility in some situations. While the LED proposal stated that the purpose of processing should be explicitly shown in the logs; the final version requires instead that it should 'possible to establish the *justification*' [emphasis added] from them. The final version states that it should be possible to establish the recipients of personal data, a requirement absent from explicit requirements in the proposal. It further added an obligation to make logs available to supervisory authorities on request.

A significant legal change in relation to logging occurs beyond Article 25 LED. Concerned with the cost of adding logging facilities to existing automated systems, the Council at first reading added provisions extending permitted transposition time for certain systems. Where systems were introduced before the Directive became applicable and introducing logging would involve disproportionate effort, Member States may delay the introduction of logging until May 2023, a period which may be extended to May 2026 for any system where introducing logging would 'cause serious difficulties for [its] operation', subject to notification of these reasons to the Commission.[26] The recitals state that controllers availing themselves of these extensions must still use 'effective methods' in the interim period to demonstrate the legality of their processing.[27]

In contrast to the LED, logging is not a requirement in the GDPR. It may however be an optional way to contribute to compliance with the security principle. Controllers are responsible for assessing whether the risks of maintaining such a log, which constitutes a form of workplace surveillance and may create risks of leakage, are justified in light of the risks posed by lack of detailed oversight over the processing system in question.[28]

[24] Art. 24 LED Proposal.
[25] Art. 2(2) LED.
[26] Art. 63(2) and (3) LED.
[27] Rec. 96 LED.
[28] CNIL 2021.

Select other EU legal instruments that were passed at the same time or since the LED which provide for logging obligations and restrict their usage, such as the Europol Regulation,[29] the ETIAS Regulation,[30] and the SIS Regulation[31] do not permit logs to be used for criminal proceedings as the LED does. The LED construction is however repeated in the EPPO Regulation, which permits such use; a choice likely grounded in the prosecutorial role of that office.[32]

Logging is a requirement placed upon users and providers of "high-risk" systems in the Artificial Intelligence Act Proposal.[33] Competent authorities would often be 'users' of these systems, including when they are profiling data subjects using AI systems pursuant to the definition of profiling in the LED.[34] Proposed logging requirements would go beyond the LED in specific situations, such as requiring the recording of two natural persons to confirm a match when using a real-time biometric identification system. Obligations to facilitate such logging would also be placed on providers of these systems on the Union market.[35] In the related AI Liability Directive Proposal, disclosure provisions applicable to logging are intended to interact with the design requirements.[36]

2. International instruments

Interpol's Rules on the Processing of Data contain logging requirements applicable to the General Secretariat, referred to as a 'Register of Processing Operations'.[37] This includes logging access, erasure, retention, updating, recording, consultation and requests for data. These follow on from logging provisions in earlier Interpol instruments, including, *inter alia*, the Rules on the Processing of Information for the Purposes of International Police Co-operation and their associated Implementing Rules.[38] However, unlike the LED,

[29] Art. 40 Europol Regulation 2016.
[30] Art. 70 ETIAS Regulation 2018.
[31] Arts. 12 and 18 SIS Regulation 2018.
[32] Art. 69 EPPO Regulation 2017.
[33] Arts. 12(4) and 14(5) Artificial Intelligence Act Proposal 2021.
[34] Art. 3(4) LED; Artificial Intelligence Act Proposal 2021, annex III para. 6(e) and (f).
[35] Art. 12 Artificial Intelligence Act Proposal.
[36] Recs. 16, 27 and Art. 3 AI Liability Directive Proposal.
[37] Art. 126 Interpol 2019.
[38] Art. 20(1)(b) Interpol 2003.

Interpol's logs may not be checked for the purpose of criminal investigations, except those related to compliance with the Rules.[39]

Insofar as logging contributes to operational security practices, DPAs have to date placed weight on international technical standards in order to interpret logging requirements in instruments other than the Directive, in particular the International Organization for Standardization's ISO/IEC 27002.[40]

3. National legislation

The WP29 expected national implementations of the LED to elaborate logging requirements, including regarding content, storage periods, technical measures including those guaranteeing log integrity, self-auditing and internal compliance-promoting policies.[41] However, only limited implementation differences have been highlighted in the literature.[42]

Member States do vary in relation to how they establish storage limitations on logs. Some specify a time limit in national law. In Greece and Germany, this is the end of the year following the year the logs were generated.[43] In Italy is it set in in further presidential decrees.[44] Some, like Estonia, explicitly leave it up to the data controller.[45] Others have issued (or may yet still issue) guidance from their supervisory authorities. For example, the CNIL recommends the retention period last between six months and one year, although recognises that there may be security reasons to keep data beyond this length if justified.[46] The CNIL emphasises in this guidance that it is not possible to justify the retention of logging data by reference to the length of the statute of limitations related to the prosecution of those who may misuse this data.

[39] Arts. 13(e) and 126(5) Interpol 2019.
[40] See e.g., College bescherming persoonsgegevens (Dutch DPA) 2015, section 3.5. This document refers to section 12.4 of the 2013 standard; this corresponds to section 8.15 of the now-updated ISO/IEC 27002 2022.
[41] WP29 2017 A, p. 26.
[42] See e.g., Hudobnik 2020 (comparing IE, UK, DE and AT).
[43] Art. 74(4) Greek Data Protection Act; German Federal Data Protection Act, s. 76(4).
[44] Art. 21 Italian LED Implementing Act.
[45] Estonian Personal Data Protection Law, s, 36.
[46] CNIL 2021.

Few national implementations have gone beyond the LED in relation to logging. Notably, while in the LED (unlike the Draft LED), logging is only for automated systems, but Austria in particular has extended this to include manual processing operations, at least ‘queries and disclosures including transmissions, changes and deletions’.[47] Typically however, this author has found that the logging requirements in the LED have been transposed relatively literally. Precedent indicates that on-the-ground implementation may vary significantly however — the implementation of the SIS II logging requirements has significantly varied among Member States, particularly in relation to what is logged, for how long logs are retained, and functionality available to analyse logs.[48] At the time of writing, the UK Government, now outside the EU but the only third country with an LED adequacy agreement, has proposed legislation amending its national transposition to diverge from the LED in terms of logging, removing its requirement to log ‘justification’.[49]

4. Case law

At the time of writing, there is no European case law directly relating to logging under the LED, nor are there any preliminary questions referred to the CJEU relating to either Article 25 LED or its closely connected provisions. However, case law from both the ECtHR and CJEU illuminates the nature of logging obligations under data protection more generally.

The ECtHR has found that in the medical context, states can have a positive obligation under Article 8 ECHR to ensure adequate logs are kept that allow the users accessing sensitive data to be identified. In the case of *I v. Finland*, it was not possible to retroactively establish who had used the applicant’s electronic health records, which led to the applicant being unable to establish a causal connection between the access to her health records and the misuse of her data. The ECtHR stated that:

> *‘to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital’s record keeping [..] It is plain that had the hospital provided a greater control over access to health records [..] by maintaining a log of all persons who had accessed the applicant’s medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. For the Court, what is decisive is that the records system in place in the hospital was clearly not*

[47] Austrian Data Protection Act s. 50 para. 3 (author’s translation).
[48] SIS II Supervision Coordination Group 2020.
[49] United Kingdom Data Protection Bill 2022, cl. 16.

> *in accordance with the legal requirements contained in section 26 of the Personal Files Act, a fact that was not given due weight by the domestic courts.'*[50]

While Finnish law did not specify the technique of logging as a requirement, the ECtHR effectively, and with the help of national judgments, made the link between security and this specific measure. It places emphasis on the benefit of logging for the human rights of the data subject in bringing legal action, something also emphasised by the WP29.[51]

The CJEU also characterised the nature of logging data in *Rijkeboer*.[52] Transparency rights under the GDPR can be used to request both the substantive personal data undergoing processing, which the CJEU terms 'basic data' as well as the personal data describing the processing activities, which practitioners typically term 'metadata'.[53] The latter category overlaps heavily with the types of data implicated by the LED logging requirements, such as processing purpose, time of collection and expected dates of erasure, and the identity of the data's sources or recipients, as logs are effectively just fine-grained metadata concerning data processing. The essential contestation in the *Rijkeboer* case is whether or not the controller had prematurely erased the metadata, and in doing so, undermined the transparency obligations in data protection law. The CJEU observed that while Member States could determine the retention duration for such metadata, it must ensure a 'fair balance' when doing so.[54] Unless storage would constitute an 'excessive burden' on the controller, the CJEU found that 'limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period' would not constitute a fair balance between the rights of the data subject, especially their rights to object and to bring legal proceedings, versus the burden such retention places on a controller. When the proceedings returned to the Dutch *Raad van State*, the municipality was unable to convincingly argue that retention was excessively burdensome, and the referring court consequently declared the limiting provision in national law incompatible with European law.[55] As the LED similarly does not set precise times on retention of logs, it seems a similar balancing exercise should also apply to logs kept under this regime.

[50] *I v. Finland*, Appl. No. 20511/03, para. 44.
[51] WP29 2017 A, p. 26.
[52] Case C-553/07 *Rijkeboer*.
[53] Case C-553/07 *Rijkeboer*, paras. 43, 50.
[54] See generally on fair balancing, Ausloos 2020, ch. 5.
[55] Judgment in *Raad van State*, para. 2.3.

C. Analysis

Several issues stand out in relation to logging. Below, a selection are dealt with in turn following the structure of Article 25 LED.

1. Processing operations covered by logs (Article 25(1) LED)

The LED requires logging of the processing activities of collection, alteration, consultation, disclosure (including transfers), combination and erasure. Compared to the list of terms used in the definition of processing, this excludes 'recording', 'organisation', 'structuring', 'storage', 'adaptation', 'retrieval', 'use', 'dissemination or otherwise making available', 'alignment', 'restriction' and 'destruction'.[56] Some of these obviously overlap, and there is a considerable deal of redundancy in the definition of processing. However, some omissions are notable. It is arguable that integrating data in advanced search systems, for example, falls under 'adaptation', 'organisation', 'structuring' and 'use', but may not fall under the terms covered in logging, with the potential exception of 'combination'. Furthermore, there may be times when data is 'retrieved' but not 'consulted' — perhaps that it comes up in a search result, but a user does not look at that specific record. These distinctions leave some legal uncertainty, particularly as scholars have argued it is inappropriate to consider the words used in the definition of processing as a conceptual taxonomy of processing activities that can be applied in practice.[57]

The text does not prefer the controller or the processor to keep the logs, leaving the arrangement flexible. Member State implementations have in general made this flexibility explicit. The Irish implementation, for example, states that logging obligations fall on controller or processor ('as the case may be').[58]

Extent of logging obligations

The LED's explicit logging requirement does not exhaustively cover the type of security-related logging referred to in ISO/IEC 27002. It does not maximally harmonise the area, nor even represent the totality of logging that may be implicitly required by the LED elsewhere. Article 25 LED covers interactions with personal data which might constitute processing. Its requirement to log justification and, insofar as possible, the identity of

[56] Art. 3(2) LED.
[57] Mahieu and Van Hoboken 2019.
[58] Irish Data Protection Act 2018, s. 82(1).

individuals whom personal data are consulted by or disclosed to, indicates a particular emphasis on sociotechnical security risks and 'insider attacks'. These types of logs are only one of many which are security relevant.[59] These broader categories might involve network connectivity to the servers in which personal data is held, log-in attempts, the creation of new users, escalation of privileges, or the availability of certain systems, none of which always corresponds to personal data processing. Consequently, where they are required for effective security, controllers may have further and wider logging requirements flowing independently and implicitly from the security principle in Article 4(1)(f) LED. This draws attention to the multiple rationales behind Article 25 LED.

Logging complex data analysis

It is tempting to consider the LED just in terms of a simple, if extensive, tabular database, with records being edited like a large spreadsheet. However, data processing techniques used in law enforcement are often computationally and data intensive. The German Federal DPA understands 'combination' within the context of logging to include forecasting tools based on data mining and algorithms, indicating that logging must also be able to work in systems of prediction and detailed analysis based on personal data.[60] In the context of facial recognition systems, the EDPB understands logging to include 'the outcome and confidence score', although notes that its recommendations are 'partly beyond' Article 25 LED.[61]

Retaining logs of data changes in complex and extensive data structures can be computationally difficult and costly as datasets become complex and unwieldy. The BfDI notes this in part, emphasising that as many law enforcement tools connect a huge array of datasets in relation to an entity retrieved 'a simple mouse click', the log entries created from this can become 'unmanageable'. There are two aspects to this unmanageability. The first is the volume of data becoming difficult to parse for the purposes of accountability. To this end, the BfDI note that the 'traceability of such logging can only be achieved with a suitable graphical evaluation tool', and that logging should therefore 'be able to visually display differences in different versions of networks' over time in order to make them interpretable to supervisory authorities.[62] Competent authorities may be

[59] See eg ISO/IEC 27002:2022, s. 18.5.
[60] BfDI 2021, p.7.
[61] EDPB 2022, para. 100.
[62] Ibid., p.9.

supported in this, at least for AI systems, with the logging design requirements placed upon providers in the proposed Artificial Intelligence Act.[63]

The second aspect of unmanageability concerns logging data size. If an organisation wished to record all changes to a dataset such that the dataset itself could be 'rolled back' to see who changed what and when, this would be a form of version control which is complex to computationally implement, can occupy a large amount of file space (particularly for complex data formats), and can corrupt data if implemented incorrectly. However, if the purpose of the log is simply to record that 'a' change was made, rather than specify the nature of that change in a replicable way, this would not come with these downsides. It would, however, be harder to use for the purposes of accountability. The text is unclear on which side to lean on here — it states that logs should be kept for certain operations, and that logging should make it establish facts concerning those operations, but it does not state how much detail on the operation itself must be stored in these logs. The EDPB, in draft guidance on facial recognition systems for law enforcement, recommend logging any changes to underlying reference databases, including to 'keep a copy of the relevant (added, deleted or updated) image, when it is not otherwise possible to verify the lawfulness or the outcome of the processing operations'.[64] It seems that controllers may find themselves having to analyse exactly how much of the story of personal data processing can and should be rebuildable from the logs — a balance which is likely to require case-by-case on which the LED provides scant guidance.

2. Purpose and use of logs (Article 25(2) LED)

The LED requires logs collected under Article 25 to be used 'solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings'. This leaves some questions open as to the breadth of activities that can fit under this umbrella.

Criminal proceedings

Some guidance indicates that such criminal proceedings must necessarily relate to criminal misuse of data, such a data breach, as is the guidance of the WP29 and the BfDI, and in parallel, in Interpol's rules on the processing of data.[65] However, the wording of the article remains open-ended. This indicates that the LED may open up the possibility

[63] Art. 12 Artificial Intelligence Act Proposal 2021.
[64] EDPB 2022, para. 100.
[65] Interpol 2019; WP29 2017 A, p.27; BfDI 2021, p.3.

to use logs in criminal proceedings unrelated to data breaches and similar events. An imaginable example would be to generate evidence about when particular users were online and accessing a system to provide information about their whereabouts, rather than intrinsically about the processing activities in question.

Employee surveillance and algorithmic management

Logging is a case of mixed data, relating both to workers as data subjects engaging in activity being logged, and data subjects to whom the data within the law enforcement processing system relate. The CNIL states that employees must be informed of the existence of the logging system, the nature of the data collected, and its retention period.[66] In general, logging raises concerns around employee surveillance.[67] However, Article 25(2) LED provides an exhaustive list of processing purposes for which the logging mandated by this Article can be used. No further purposes, such as employee appraisal or algorithmic management are permitted. Workers using the logging system who wish to exercise data rights in relation to it, such as the right of access, would seem to have to rely on rights as they manifest in the LED, which in general are more limited and restricted than those in the GDPR which they have access to for other data held by their employer.

However, the LED does not apply to all data processing undertaken by competent authorities. For example, human resources processing within a police department, and any related logging, would trigger the GDPR framework instead.[68] Furthermore, Article 25 LED does not cover all logging that a competent authority may need to, or may wish to, implement.[69] A grey area therefore exists around prohibitions on use for additional logging. It would seem that the scope for workplace surveillance of individuals within a competent authority is broader where an individual is using a system which is not related to an LED processing purpose, or potentially where logging beyond that mandated in Article 25 LED is applied.

Disclosure of logs to data subjects

Data subjects have rights under the LED to obtain from the controller 'the recipients or categories of recipients to whom the personal data have been disclosed'.[70] This aspect of the law remains ambiguous. Empirically, controllers, in the framework of the GDPR, often

[66] CNIL 2021, p. 2.
[67] See generally WP29 2017 B.
[68] Rec. 11, LED.
[69] See further section C.1. above.
[70] Art. 14(c) LED.

return *categories* of recipients rather than specific recipients as a result.[71] In the GDPR, this makes it difficult to follow the provenance of data processing, as only reliable backward provenance (knowing where data came from), rather than forward provenance (concerning where the data went), is clearly possible.[72] In the LED, this leaves an even greater vacuum, as there are no obligations to provide the source of personal data to data subjects, likely to ensure those sources' protection.

The logging requirement in the LED mandates that information on specific recipients be retained. It follows that, in line with the fairness principle, a controller could not refuse to provide this information on this basis, given that retention has been undertaken and such data exists. Use of logs in this manner appears compatible with the exhaustive list of purposes of Article 25 LED, as one purpose of data access requests is to verify the legality of processing.[73] This is not to say that this alone would oblige information be provided; controllers could still rely on the limitations to this right to justify occasions where it would not be in the public interest to release this information, although they may have to provide the data to a DPA for analysis in lieu of the data subject.[74]

3. Making available to supervisory authority (Article 25(3) LED)

On a first glance, Article 25(3) LED provides little beyond the powers already entrusted to supervisory authorities in the LED to 'obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks'.[75] Supervisory authorities 'on request' can approach either the controller or the processor for logs. The barrier for the use of these powers is low; no investigation or similar needs to be underway for logs to be provided. As a consequence, it is possible that regular review of logs could form a simple precursor step to triage further action, similar to how authorities make use of DPIAs where they exist as a form of 'meta-regulation'.[76]

Continuous review

[71] Mahieu, Asghari, and van Eeten 2018; cf. WP29 2018, p. 37 (stating, in relation to the GDPR, that controllers must provide the information on recipients that is most 'meaningful' to data subjects, and their ability to 'opt' to provide only categories must be understood specifically within that framework.)

[72] This is due to the obligation to provide information as to the source of data, Arts. 14(2)(f), 15(1)(g) GDPR. See generally Veale et al. 2018.

[73] Rec. 43 LED.

[74] Art. 15 LED.

[75] Art. 47(1) LED.

[76] Binns 2017.

Some commentators have highlighted the absence of a need to regularly review logs to monitor compliance and address shortcomings.[77] This is absent from Article 25 LED more broadly, although such obligations on both controllers and processors may be implicit in particular in the ‘technical and organisational measures’ required to ensure security and compliance with data protection by design.[78]

[77] Vogiatzouglou and Marquenie 2022, p. 79.

[78] Arts. 19(1), 20, 22(1), 29(1) LED. See the commentaries on Arts. 20 & 29 in this volume.

Bibliography

International agreements

Interpol 2003: Interpol, ‘Rules on the Processing of Information for the Purposes of International Police Co-operation’ (2003).

Interpol 2019: Interpol, ‘Rules on the Processing of Data’ (2019).

EU legislation

CIS Convention 1995: Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, OJ 1995 C316/34, 27 November 1995.

CISA 2000: Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ 2000 L239/19, 22 September 2000.

SIS II Decision 2007: Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205/63.

Europol Regulation 2016: 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) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135/53.

EPPO Regulation 2017: Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ 2017 L283/1.

ETIAS Regulation 2018: Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, OJ 2018 L236/1.

SIS Regulation 2018: Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, OJ L236/1.

Artificial Intelligence Act Proposal 2021: European Commission, ‘Proposal for a Regulation of the Parliament and of the Council Laying down Harmonised Rules on Artificial

Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts', COM(2021) 206 final, 21 April 2021.

AI Liability Directive Proposal 2022: European Commission, 'Proposal for a Directive of the Parliament and the Council adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)', COM(2022) 496 final, 28 September 2022.

National legislation

Austrian Federal Data Protection Act: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz— DSG), BGBl. I Nr. 165/ 1999 zuletzt geändert durch BGBl. I Nr. 24/ 2018.

Estonian Personal Data Protection Law: *Isikuandmete kaitse seadus*, RT I, 4 January 2019, 11.

German Federal Data Protection Act 2017: Bundesdatenschutzgesetz vom 30. Juni 2017, BGBl. 2017 Teil I Nr. 2097.LED

Greek Data Protection Act of 2019: Hellenic Data Protection Authority (HDPA), measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Government Gazette of the Hellenic Republic Issue No. 137, Law No. 4624, 29 August 2019.

Italian LED Implementing Act: *Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del* 27.4.2016. GU n.119, 24 May 2018.

Irish Data Protection Act 2018: Data Protection Act 2018 (7/2018)

United Kingdom Data Protection Bill 2022: Data Protection and Digital Information Bill, Bill 143 2022-23 (as introduced).

Academic writings

Ausloos 2020: Ausloos, *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection* (OUP 2020).

Ausloos and Dewitte 2018: Ausloos and Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice', 8 *International Data Privacy Law* (2018), 4.

Binns 2017: Binns, 'Data protection impact assessments: a meta-regulatory approach', 7 *International Data Privacy Law* (2017), 22.

Hudobnik 2020: Hudobnik, ‘Data Protection and the Law Enforcement Directive: A Procrustean Bed across Europe?’, 21 *ERA Forum* (2020), 485.

Mahieu, Asghari, and van Eeten 2018: Mahieu, Asghari, and van Eeten, ‘Collectively Exercising the Right of Access: Individual Effort, Societal Effect’, 7(3) *Internet Policy Review* (2018).

Mahieu and Van Hoboken 2019: Mahieu and Van Hoboken, ‘Fashion-ID: Introducing a Phase-Oriented Approach to Data Protection?’ (*European Law Blog*, 30 September 2019).

Purtova 2018: Purtova, ‘Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships’, 8 International Data Privacy Law (2018), 1.

Veale et al. 2018: Veale, Edwards, Eyers, Henderson, Millard, Lerner, ‘Automating Data Rights’, in David Eyers, Christopher Millard, Margo Seltzer, and Jatinder Singh (eds.), *Towards Accountable Systems: Report from Dagstuhl Seminar 18181* (Dagstuhl Publishing 2018).

Papers of data protection authorities

WP29 2017 A: Article 29 Working Party, ‘Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)’ (WP 258, 29 November 2017a).

WP29 2017 B: Article 29 Working Party, ‘Opinion 2/2017 on data processing at work’ (WP 249, 8 June 2017b).

WP29 2018: Article 29 Working Party, ‘Guidelines on transparency under Regulation 2016/679’ (WP260 rev.01, 11 April 2018).

BfDI 2021: Federal Commissioner for Data Protection and Freedom of Information (BfDI), ‘Hinweise zu den datenschutzrechtlichen Anforderungen an die Protokollierung nach § 76 Bundesdatenschutzgesetz’ (23 March 2021).

CNIL 2021: CNIL, ‘Délibération no 2021-122 du 14 octobre 2021 portant adoption d’une recommandation relative à la journalisation’, Journal Officiel de La République Française n° 0254 (30 October 2021).

College bescherming persoonsgegevens 2015: College bescherming persoonsgegevens, ‘Onderzoek beveiliging SIS II bij de Nederlandse Politie, openbare versie’ (Z2015-00126, 2015).

EDPB 2022: European Data Protection Board, ‘Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version for public consultation’ (12 May 2022).

EDPS 2006: European Data Protection Supervisor, ‘Comments of the European Data Protection Supervisor on the recent developments with respect to the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters’ (16 November 2006).

Reports and recommendations

ISO/IEC 27002:2022: International Organization for Standardization (ISO) ‘Information technology — Security techniques — Code of practice for information security controls’ (ISO/IEC 27002:2022) (2022).

SIS II Supervision Coordination Group 2020: SIS II Supervision Coordination Group ‘Report on logging to the SIS II at national level’ (1 July 2020).

Vogiatzoglou and Marquenie 2022: "Vogiatzoglou and Marquenie, ‘Assessment of the Implementation of the Law Enforcement Directive’ (study commissioned by the European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs at the request of the Committee on Civil Liberties, Justice and Home Affairs; PE 740.209, December 2022)

Council Position 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 2016 C158/46.

Others

European Parliament 2008: European Parliament legislative resolution of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, P6_TA(2008)0436.

Tweedekamer 2021: Aanhangsel Handelingen II 2020/21, nr. 1377 (Netherlands).