Legal Tech vs Data in Organisation

Małgorzata Kurowska

1. Data vs Information

Both data and information are concepts understood intuitively in everyday life and, as experience has shown, also interchangeably, even by lawyers. However, information security management methodologies treat these concepts separately, with such distinction being crucial from the point of view of proper modelling of the information management process in a law firm.

Currently, ISO standards of the 27 000 family of standards (Information Security Management) do not define information. This concept is defined in a slightly different context in the ISO 2832:2015 framework defining key definitions in the field of information technology which takes, as central, the concept of information, understood as:

> *"Knowledge concerning any objects such as facts, events, things, processes or ideas including concepts that within a certain context have a particular meaning."*[1]

The concept of data is derived from information and is defined as:

> *"A reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing"*[2]

Legal scholars and commentators formulate definitions of the above-mentioned concepts on the grounds of legal scholarship and writings generally draw on an analogous distinction, assuming that data are fixed (recorded) signs that – at least for some time – are potentially interpretable[3]. Viewed as such, **information is the result of data interpretation**.

---

1 <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en> access 12 January 2021.

2 ibid.

3 D. Szostek, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej (1st edn, Legalis 2012) [New treatment of a document in Polish private law with particular reference to a document in electronic form].

Information is therefore subjective in nature[4]. It cannot therefore be protected as such and, in order to respect legal certainty, we must ensure that data is protected as potentially interpretable.

This results in a number of normative **divisions of data** according to the type of information that can be decoded from such data. Just to mention in passing, it is worth pointing out that such divisions are based on inconsistent nomenclature and do not always take into account the distinction described above between information and data.

From a practical perspective, the most typical divisions that are of relevance to a lawyer, are as follows:

1) **personal data and non-personal data**

The GDPR defines personal data as *any information relating to an identified or identifiable natural person (...)*[5]. As can be seen, the definition itself uses the concepts of data and information interchangeably. In this regard, the prevailing view among legal scholars and commentators[6] is that personal data is a subjective concept, and that the nature of data as personal data depends on the degree of identifiability of a natural person in light of a reasonable likelihood of such identification (cf. recital 26 of the GDPR).

The definition of non-personal data is even more succinct. The EU Non-Personal Data Regulation[7] defines data subject to the Regulation simply as data other than personal data as defined in Article 4(1) of Regulation (EU) 2016/679 (Article 3(1)).

Thus, the European legislator assumes a dual division – however, it is difficult to determine at first sight whether this division refers to information (data interpreted as relating to a natural person, i.e. personal data and data which cannot be so interpreted), or to data as such (according to this approach, the non-personal data regulation would refer both to data which cannot be interpreted as personal data ("non-personal information") and to any data, including data which is not information at all.

---

4 D. Szostek, (3).

5 General Data Protection Regulation, art. 4(1).

6 P. Litwiński (ed.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. EU Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (C. H. Beck 2018) marginal numbers 21-23; cf. also Lee A. Bygrave and Luca Tosoni, 'Commentary on Article 4' in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds) *The EU General Data Protection Regulation (GDPR). A Commentary* (OUP 2020).

7 Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59..

Despite the above inconsistency, the latter approach should be supported, and it should be considered that, in light of the objectives of the non-personal data regulation, the intention of the European legislator was to ensure the protection of **data** flows, regardless of whether and under what circumstances they are interpreted in a way that gives them meaning (legal, business, economic or social).

2) **information covered by professional secrecy and information not covered by professional secrecy**

The Code of Conduct for European Lawyers does not define professional secrecy as such. However, it provides a description of the elements that information covered by such secrecy should meet[8]. However, professional secrecy is defined in a number of corporate regulations of EU Member States.

For example, according to the **Polish** Code of Ethics of Attorneys at Law (KERP):

(...) Attorneys at law shall keep secret all information about the client and their affairs, whether disclosed by the client or obtained in any other manner in connection with the performance of any of their professional duties and regardless of the source of such information or the form and manner of its recording (professional secrecy)[9].

Further, KERP specifies that professional secrecy extends to documents and correspondence drafted or exchanged in connection with the provision of legal assistance.

In contrast, the **French regulation** relating to the profession of lawyer (*Règlement Intérierur National de la Profession d'Avocat, RIN*) provides that:

Professional secrecy covers all matters in connection with the provision of legal advice or defence, whether recorded on a tangible or intangible medium (hard copy, fax, electronic form)[10]. RIN also sets out a broad, open-ended catalogue of information covered by the confidentiality obligation.

Similarly, **the German law on the practice of a legal profession** (BRAO)[11] defines professional secrecy as anything learned in the course of the practice of a legal profession (Article 43a(2) BRAO).

---

8 Chapter 2.3: <https://www.brrp.pl/pdf/Kodeks_Etyki_Prawnik%C3%B3w_Europejskich.pdf> accessed 12 January 2021.

9 Article 15: <https://kirp.pl/etyka-i-wykonywanie-zawodu/etyka/kodeks-etyki-radcy-prawnego/> accessed 12 January 2021.

10 Art 2: <https://www.cnb.avocat.fr/sites/default/files/rin_2020-11-30_consolidefinal.pdf> accessed 12 January 2021.

11 <https://www.gesetze-im-internet.de/brao/> accessed 12 January 2021.

These – and other – legal divisions of information focus on the protective function, while defining the framework for handling information generally at a level other than strictly personal. Establishing to which category or categories the information belongs and, consequently, what legal and ethical requirements a lawyer should meet, is a basic condition for proper information security management[12].

2. *Information Classification as an Information Security Tool*

Information classification can be based on different criteria, depending on its purpose. In general, information division in an organisation refers to the potential consequences of a breach of information confidentiality (understood as a situation where information is disclosed to an unauthorised person). The consequences of such a potential breach may be, in particular, regulatory (in the sense of legal capacity to continue operations in the event of a breach), financial or reputational[13].

Information classification in an organisation allows for a structured and accountable application of consistent security policies defined at the organisation level for specific classes of information.

However, the processing of information by the Law Firm involves lawyer's liability in a number of aspects. As regards LegalTech tools, that are generally less recognised and require technical competence on the part of a lawyer, the same is required to exercise utmost care in implementing them and ensuring security of use. As we shall see later in this section, failure to exercise due diligence – corresponding to the professional nature of the activity pursued, and of particular social importance – exposes a lawyer to disciplinary liability. The need to demonstrate due diligence (accountability) may be responded to by a security-by-design (or "secure-by-design") approach.

12 As per clause A 7.2 of Annex A of ISO 27 001, the purpose of information classification is to *ensure that information receives the appropriate level of protection*. For more details, see section Legal Tech vs Data in Organisation.

13 The ISO 31000 standard provides such examples as financial aspects, impact on safety and hygiene, or environmental impact. From the perspective of practising as an attorney at law / advocate, the consequences for the security of professional secrecy and the continuity of providing legal services may be of significant importance. For more information, see section Legal Tech vs Data in Organisation.

The security-by-design approach is used primarily in the context of designing IT solutions[14] or in the broader sense of Enterprise Security Risks Management[15]. The security-by-design approach, viewed as such, is a concept to ensure the ongoing management of security risks that change over time, taking into account the specific aspects of an organisation.

Information security management is modelled on the traditional Deming cycle (Plan-Do-Check-Act)[16]. However, security-by-design focuses primarily on the **objectives** of the security solutions implemented rather than on the specific tools that provide them, which naturally follow from the objectives and assumptions adopted[17].

As mentioned, the concept of security-by-design refers to the management of security in an organisation; however, some of its assumptions perfectly reflect the suggestions related to the implementation of new LegalTech solutions in an organisation. These assumptions include in particular:

- **Security culture**

Suggestion that the organisation's management constantly build awareness of the importance of safety (tone from the top) and ensure transparent communication about safety standards and expectations.

- **Designing solutions that do not become obsolete over time**

Demand for designing solutions whose main assumptions and structure remain independent of technical methods of achieving the objective, i.e. solutions that are capable of initiating technical solutions rather than those that depend on the existing solutions.

- **Continuous (ongoing) monitoring and improvement**

Suggestion that the process is not aimed at achieving a certain level of security, but rather at achieving and maintaining it, i.e. activities that require flexible adaptation to ongoing changes in external and internal conditions.

The development of LegalTech solutions, due to the importance of the information processed with their use and the associated responsibilities,

14 Cf. Wikipedia, 'Secure by design' <https://en.wikipedia.org/wiki/Secure_by_design> accessed 13 January 2021.

15 Cf. L. Kent Howard, 'Security by Design' (2019) 12(2) Journal of Physical Security 1-13.

16 ISO/IEC 27001:2005.

17 Howard (n 15).

requires lawyers using them to understand how such solutions work and what their limitations are[18]. The chapter *Legal Tech vs Data in Organisation* further describes the suggested practical model for ensuring secure – from a legal, organisational and technical perspective – implementation and use of LegalTech solutions.

3. *Information Processing via LegalTech Tools*

The most common applications of LegalTech[19] today primarily include[20]:

- **e-discovery solutions**; in this context, it seems that the understanding of the term LegalTech is somewhat expanded to include the automated analysis of legal texts not only in relation to court proceedings, especially on the grounds of precedent law, for which such solutions were originally developed, but also to review of documents while providing services relating to due diligence or audit proceedings;
- solutions to support the creation of **standardised and consistent templates for legal documents**;
- **client support tools** – such as platforms that facilitate the purchase of legal services[21].

From a legal perspective, the purpose of information processing within a solution is of paramount importance. To a large extent, it is the very purpose of the processing that will determine the admissibility of using a particular tool (legal basis to use information from a particular source for a particular purpose), the scope of information used (e.g. obligation to minimise the personal data processed) or the scope of liability related

18 CCBE, *Considerations on the legal aspects of artificial intelligence*, (2020) <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf> accessed 12 January 2021.

19 Because of the profile, the use of LegalTech tools in court has been omitted; interesting conclusions on the topic are available in the study entitled CCBE (n 18).

20 CCBE Considerations (n 18).

21 Solutions that enable the client-consumer to resolve legal issues on their own (directly), without lawyer's assistance, are sometimes placed outside the concept of LegalTech, and are classified in a separate category: LawTech [cf. Susana Navas, 'LegalTech Services and the Digital Content and Digital Services Directive', 6<https://www.academia.edu/44791640/LegalTech_Services_and_the_Digital_Content_and_Digital_Services_Directive> accessed 12 January 2021.

to the processing (liability regime related to personal data, liability for ensuring the confidentiality of business or professional secrecy.

4. *Liability for Data Security*

A lawyer's liability for the consequences of an information security breach (in particular, its loss or disclosure to unauthorised persons) may be considered on civil, administrative, criminal and disciplinary grounds.

Civil law and administrative law solutions related to data breaches are relatively uniform across the EU countries since they are governed, to a considerable extent, by a regulation of the Council and the European Parliament. The GDPR provides for both the possibility of imposing financial administrative sanctions by the competent supervisory authority, both financial (Article 83 GDPR) and non-financial sanctions (reprimand, order for specific action – Article 58 GDPR).

In turn, Article 82 GDPR concerns the possibility for an individual who has suffered damage relating to a breach to bring a claim for damages against the data controller or processor. Damage is understood here in a broad sense and includes both material and non-material damage[22].

Detailed rules for pursuing claims are governed by national legislation, providing for interesting derogations in certain cases. As an illustration, the French law on information processing, data filing systems and related freedoms[23] provides in its Article 37 the possibility for a class action (*action de groupe*) to be brought by all persons affected by a similar type of damage resulting from the same breach of data protection rules. In turn, the provisions of Polish law explicitly exclude the vast majority of claims for infringement of personal interests from class actions, which will effectively exclude some personal data claims[24]

---

22 Gabriela Zanfir-Fortuna, 'Commentary to Article 82' in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds) The EU General Data Protection Regulation (GDPR). A Commentary (OUP 2020) 1175.

23 1978, La loi relative à l'informatique, aux fichiers et aux libertés nº 78-17 du 6 janvier 1978 , <www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/2021-01-12/> accessed 12 January 2021.

24 Cf. Article 1(2a), Act on Pursuing Claims in Class Actions,Journal of Laws of 2020, item 446, in conjunction with Article 92, Act on the Protection of Personal Data, i.e. Journal of Laws of 2019, item 1781; it is worth mentioning here that the Polish Supreme Court generally accepts that the protection of personal data and personal interests constitute two separate protection regimes, which, however, may overlap in certain cases (cf. B. Łukańko, Uchybienie przepisom o ochronie

This naturally begs for the question regarding the extent of a lawyer's (Law Firm's) civil liability for damages caused by the use of LegalTech tools.

As it has already been mentioned, currently the most common LegalTech solutions used in law firms are tools supporting legal research and simple analytics. Potential damage caused by the malfunction of such tools would therefore be extremely difficult to prove, both in terms of causation and amount.

However, as the complexity of the solutions increases, the issue of liability for such damage will become increasingly important – it is enough to imagine relying on automated solutions for drafting pleadings, deciding on pleading strategy or reviewing a particular judge's decisions.

In this context, leading proposals are currently being identified to regulate the liability regime as either (1) tort liability based on fault or (2) strict liability based on, similar to a dangerous product liability regime[25]. This issue goes beyond the limits of this paper; however, it is worth bearing in mind that it should be resolved taking into account issues such as a lawyer's duty of care. In the case of a lawyer, such care should extend to the entire process of implementing and using LegalTech solutions, from reviewing and classifying the information processed by their use, through estimating the risk associated with implementing the solution, appropriate training, to deciding how to work with those involved in the information processing.

From the perspective of these considerations, it is also necessary to mention the consequences related to the breach of security of not so much personal data, but rather of information constituting professional secrecy (attorney at law's or advocate's secrecy), consisting in its loss or compromise to its confidentiality or integrity. Given the definition of professional secrecy, which is uniformly extremely broad, the vast majority of personal data breaches generally also amount to breaches of professional secrecy. The data protection regime shall be complementary to the duty of confidentiality[26].

Breach of professional secrecy primarily gives rise to a lawyer's disciplinary and criminal liability.

---

danych osobowych jako naruszenie dobra osobistego – analiza na przykładzie orzecznictwa Sądu Najwyższego (2016) 46 UWM, Studia Prawnoustrojowe, .

25 CCBE Considerations (18) 25; cf. Martin Ebers, Susana Navas, Algorithms and law (UCL 2020).

26 CCBE Considerations (18) 33.

Professional secrecy is one of the key ethical principles and the essence of a lawyer's activity (cf. section 2.3.1. of the Code of Conduct for European Lawyers) and lies at the core of a lawyer's ethical obligations[27]. It is accepted that *professional secrecy is an interest in itself, as an element of the proper and ethical exercise of the profession*[28], and even that it is an intrinsic condition of the exercise of a legal profession[29]. The obligation to preserve professional secrecy implies an obligation to apply appropriate security measures in connection with the processing of information subject to it[30]. Consequently, a breach of professional secrecy (especially involving the unauthorised disclosure of information covered by secrecy) is therefore one of the most serious disciplinary offences.

5. France

Violation of legal and professional rules (including the rules of advocates' code of conduct) may result in disciplinary proceedings[31]. Potential sanctions include, in the first place, a notice, a reprimand, temporary suspension of licence to practise law and, ultimately, disbarment.

Breach of professional secrecy as such is furthermore a criminal offence. Pursuant to 226-13 of the French Criminal Code[32], disclosure of information covered by professional secrecy by a person in possession of such information, whether by virtue of a legal provision or their function, is punishable by imprisonment or a fine of up to EUR 15,000. The manner or circumstances in which the secret is disclosed are irrelevant, unless one of the exceptions set out in Article 226-14 of the Code applies.

---

27 ibid.

28 SDI 32/12, Polish Supreme Court judgement of 15 November 2012.

29 <https://actu.dalloz-etudiant.fr/fileadmin/actualites/pdfs/Porteron-_AJ_Penal_-_04052010.pdf> accessed 27 January 2021.

30 WO-106/19; Judgement of the Polish Higher Disciplinary Court of the National Bar Association of Attorneys at Law of 23 October 2019.

31 Décret n°91-1197 du 27 novembre 1991 organisant la profession d'avocat, <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000356568/2021-01-13/> accessed 13 January 2021, Article 183.

32 Code penal, <https://www.legifrance.gouv.fr/codes/id/LEGIARTI000006417945/2012-12-11/> accessed 13 January 2021.

6. Poland

The disciplinary liability of attorneys at law and advocates is set out in the Act on Attorneys at Law[33] and the Act on Advocates[34], respectively. The disciplinary court may sanction an attorney at law or an advocate sanctions such as a notice, a reprimand, a fine, as well as suspend their licence to practise law or disbar them.

The Polish Criminal Code addresses the issue in a similar manner, albeit to a broader extent. Article 266 of the Criminal Code provides for a fine, a community sentence or a sentence of imprisonment for a maximum term of two years, both in the case of unauthorised disclosure and **use** of information entrusted in connection with the performance of a function or activity.

7. Germany

The German Act on the Legal Profession provides for disciplinary liability for breach of duties under the Act (Article 113 BRAO). Confidentiality obligations are further underlined in the Rules of Professional Practice (Berufsordnung für Rechtsanwälte, BORA)[35], in its Article 2. Potential sanctions for violations of the rules of conduct include, in particular, a notice, a reprimand, a fine, suspension of a licence to practise law and disbarment (Article 114 BRAO).

Finally, the German Criminal Code (Strafgesetzbuch, StGb)[36] provides for a sentence of imprisonment for a maximum term of one year or a fine if information entrusted to the holder of a secret is disclosed in connection with his or her function or profession (Article 203 StGb). Lawyers (Rechtsanwalts) are explicitly referred to in the provision as falling within the subjective scope of the legal norm. It is worth noting here that Article 203 StGb clearly excludes sanctions for the disclosure of information covered by the service provider's secrecy if such provider's participation is necessary for the performance of certain professional activities.

---

33 The Act on Attorneys at Law, Journal of Laws of 2020, item 75, chapter 6.

34 The Act on Advocates, Journal of Laws of 2020, item 1651, chapter VIII.

35 <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/National_Regulations/DEON_National_CoC/EN_Germany_BORA_Rules_of_Professional_Practice.pdf> accessed 13 January 2021.

36 <https://www.gesetze-im-internet.de/stgb> accessed 13 January 2021.

8. Conclusion

LegalTech tools significantly contribute to making a lawyer's work simpler. When properly applied, they also improve the quality of work and, consequently, of legal services provided to clients.

Implementation of LegalTech technical solutions requires a lawyer to exercise due diligence appropriate to the profession (professional due diligence), including, in particular, to have a good capture of the tool's functionality, risk analysis and identification of risk mitigation methods. These activities should be implemented in a way that ensures accountability at every stage of the process.

Indeed, a lawyer should be mindful of the core values of the profession, i.e. protection of professional secrecy and promotion of trust between client and lawyer. Failure to comply with the fundamental obligations in terms of risk assessment and ensuring the security of processed information, coupled with compromising core values associated with the practice of the profession, may trigger a lawyer's liability – both civil liability for damages and liability under corporate control (disciplinary liability). In certain cases, a lawyer may also be held criminally liable.