DATA MATTERS

HITACHI
Inspire the Next

Managing Personal Data of Costumers and Staff — also in Respect to Designing new Products and Services — Becomes a Key Duty for C-Level Executives

EXECUTIVE LEGAL BRIEFING SERIES

New Trends in European Privacy Law 1

Transatlantic Data Flows, Hidden Risks, and Looking Ahead to Privacy Compliant Artificial Intelligence

By Victor Alexander de Pous
December 2020

LEGAL BRIEFING #2: Privacy Law 1

Contents

LEGAL BRIEFING #2: Privacy Law 1

Headlines

- What started as a legal innovation in the United States 130 years ago, turned into a strong human right and a comprehensive body of law in many countries worldwide: the right to privacy. In a digital world, the legal protection of individuals in relation to the *processing of their personal data* forms the major part of this fundamental right. For every organization in Europe and for most foreign entities that have links to an EU Member State, the General Data Protection Regulation (GDPR) is key legislation. However, in order to protect their own legitimate interests optimally, those organization need to place this European law in a broader perspective, because corporate data includes other information than personal data, and the GDPR is not the only law that applies to corporate data.

- In the past, technical knowledge has traditionally been the most relevant conditio sine qua non for the design of electronic data processing systems, but this Leitmotiv has gradually broadened to include organizational science. Subsequently, those involved in the development phase of digital products and services could no longer escape a certain understanding of the legal rules for the technology itself (such as software law and cyber security measures) and other non-technical aspects of the application. Today, the urgency of a multidisciplinary approach is rapidly increasing, including ethical and societal aspects. GDPR alone bears witness to this ambiguity. After all, taken privacy by design into account, which principle includes privacy by default, is a must for every producer of a (new) business process in which personal data are processed.

Analysis

- In addition to the GDPR with its status of an EU *regulation* that becomes immediately enforceable as law in all member states simultaneously, the European Data Protection Board (EDPB) issues Guidelines, Recommendations and Best Practices on privacy matters. Both the GDPR and the work of the EDPB are focused on achieving a truly unified body of privacy law in Europe. In practice we see national data protection authorities expressly differ from their point of view, for example relating to COVID-19 measures.

- Through its Schrems II decision of 16 July 2020, the Court of Justice of the European Union shook up daily business on both sides of the Atlantic Ocean by completely invalidating the EU-U.S. Privacy Shield framework as the most convenient legal ground for data transfer. This judgement creates legal uncertainty. It is first and for all up to EU and US politics to come to terms on the amended international agreement which hopefully fully complies with the present privacy legislation and case law. Not an easy task.

- After four months there is good news. On 10 November 2020, the EDPB finally adopted (draft) recommendations on the matter of — transatlantic and other — data flows to third countries. The preferred direction is clear and with examples: deploy the co-called “Standard Contractual Clauses” or SCSs in a careful case-by-case matter. *However, in reality it probably will not always be possible to take additional measures that sufficiently protect personal data*.

- After having all the regulatory GDPR requirements in place and the corresponding continuous compliance process, organizations now face new personal data processing rules, currently under discussion. The ePrivacy Regulation will replace the outdated ePrivacy Directive, but still applies to present electronic communications (confidentiality) and digital marketing (tracking and monitoring). The new regime has to tackle the rapidly evolving technological landscape, with issues including the Internet of Things, the confidentiality of individuals’ communication on publicly accessible networks, and more.

- The complexity and extent of digital technology in organizations create additional, “off the beaten path” privacy risks which often remain invisible until an incident occurs. For example, the incorrect management of redundant domain names creates a risk for data breaches, and the same applies to operational email addresses no longer in use by an individual staff member or a department.

- A Chief Privacy Officer is not the same as a Data Protection Officer or DPO. The latter concerns a formal position with its own GDPR-based framework. Be aware that a DPO operates at least in parts independent of the management of the organization — like a supervising body — and its sometimes by law required tasks may also be executed by an external expert. Large organizations most likely need to appoint a DPO, (Chief) Privacy Officer and a Chief Information Security Officer (CISO).

- A sharp and continuous focus on the GDPR remains necessary at all times but at the same time involves the danger that other privacy laws and regulations are snowed under. Moreover, since corporate data include also other categories of data, other legal frameworks apply. Thus, a — external — audit outcome stating that a company or public sector organization is ”GDPR compliant” does not equal “privacy law compliant” and certainly not “corporate data and technology law compliant”.

Diverse and Rapidly Evolving Developments

The American lawyer and Supreme Court judge Louis Brandeis defined a new individual right in a path-breaking article he published with his partner, Samuel Warren, in the Harvard Law Review of 15 December 1890, on "The Right to Privacy." This concise, new legal concept developed over a period of 130 years into an essential and broad legal domain that touches every individual in its different capacities (citizen, consumer, employee, patient, and many more). The same applies to very organizations. Hardly any entity escapes today's privacy laws; in the European Union primarily dominated by the General Data Protection Regulation or GDPR (2016/679), which applies since 18 May 2018 and replaced the EU Privacy Directive of 1995 (95/46/EC) and the national privacy laws based thereon in all the 27 member states.

The GDPR regulates the processing of personal data *in the light of modern computing*, such as the deployment of the Internet and cloud services — indeed *in general*. Important to realize: every jurisdiction may have many other privacy-related laws enacted, both regulating specific economic sectors and/or the processing of specific types of data (e.g. financial data, healthcare data). And the European Union also makes legal distinctions.

Meanwhile, the current privacy issues are getting wider. Corona emergency measures and Corona contact and tracing apps, emerging since March 2020, may very well be predominant at this very moment but are not the only topics. Other privacy matters relate to large-scale data breaches, the use of fingerprints in the workspace, public transport chip cards, WiFi tracking and camera surveillance, connected cars, and, for example, the deployment of artificial intelligence. In the next briefing we will analyses more important decisions from courts of law and the national data protection authorities in Europe.

The Legal Battles on Transatlantic Data Flows

The GDPR provides that the transfer of personal data to a *third country* may, in principle, take place only if the third country in question ensures an adequate level of data protection. Third countries are all countries outside the EU, with the exception of the countries in the European Economic Area (EEA). These are — next to the EU member states — Norway, Liechtenstein and Iceland, and they have an equivalent level of protection of personal data. In the absence of this major condition, the law offers various alternatives.

Following discussions on the adequate level of protection in the United States, the European Commission decided that the Safe Harbour Privacy Principles, developed during 1998-2000, and ensuring sufficient protection against access by the public authorities to the data transferred to the US, did comply with the 1995 EU Privacy Directive (the Safe Harbour decision of 26 July 2000).

However, after the Austrian national Max Schrems complained in Ireland that his Facebook data were insufficiently protected, the Court of Justice of the European Union (CJEU) declared on 6 October 2015 that the Safe Harbour decision was invalid (the Schrems I decision). New talks between the EU and the US subsequently lead to "a renewed and sound framework for transatlantic data flows", based on a self-certifying system for companies in the US that they adhered to 7 privacy principles, to comply with the European privacy law.
In the Schrems II decision of 16 July 2020 the same European court, however, declared that the new international

agreement between the parties — the EU-U.S. Privacy Shield framework — is no longer a valid mechanism to transfer personal data from the European Union to the United States.

What Comes After the Schrems II Decision?

First and above all, it is up to EU and US politics to come to terms on an amended international agreement — version three. In their 10 August 2020 Joint Press Statement, European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross said that both parties "have initiated discussions" to evaluate the potential for an enhanced privacy framework. In other words, it takes time. Dutch minster for Legal Protection Sander Dekker follows the same line of thought: "Privacy Shield quick fix is complicated". Without any official guiding — neither from the European Data Protection Board (EDPB) nor the national data protection authorities in the member states — many organizations probably followed a "business-as-usual" approach, which most likely creates severe risks and liabilities.

Standard Contractual Clauses

After four months, we see light at the end of the tunnel. The EDPB closed ranks and adopted on 10 November 2020 the long-awaited — draft — recommendations on (i) measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[1], as well as (ii) recommendations on the European Essential Guarantees for surveillance measures (both are now open for public consultation until 30 November 2020). The main line is clear. The most practical solution is found in the Standard Contractual Clauses or SCSs, and by doing so "controllers are required to verify, on a *case-by-case basis* and, where appropriate, *in collaboration with the recipient of the data in the third country*, if the law of the third country ensures a level of protection of the personal data transferred that is essentially equivalent to that guaranteed in the European Economic Area (EEA)."

The European Commission can decide that SCSs offer sufficient data protection safeguards. To date three sets of those clauses have been issued. In its Schrems II ruling, the CJEU clearly held that the Commission Decision 2010/87 on SCSs for the transfer of personal data to processors established in third countries *is valid*, but with a critical note. Simply signing a SCS may not be sufficient. That validity, the CJEU adds, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honor them.

Roadmap to Data Export to Third Countries: Six Steps

The EDBP recommendations follow the route taken by the CJEU. They contain a roadmap of the steps, data exporters must take to find out if they need to put in place *supplementary measures*, to be able to transfer data outside the EEA in accordance with EU law, and help them identify those that could be effective. To assist data exporters, the recommendations also contain a non-exhaustive list of examples of supplementary measures and some of the conditions they would require to be effective. The following six steps are advised:

[1] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

1. Data exporters must know their transfers. This means that **mapping all transfers of personal data to third countries** is necessary.

2. In the second step data exporters must **verify the transfer tool** — on which the actual transfer relies on — amongst those listed under Chapter V GDPR.

3. Next in line is a **legislative assessment**. Is there anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools the data exporter is relying on, in the context of the specific transfer? This assessment should be primarily focused on third country legislation relevant to the transfer and the Article 46 GDPR transfer tool the data exporter is relying on and that may undermine its level of protection.

4. The fourth step concerns the **identification and adoption of supplementary measures** that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if the assessment reveals that the third country legislation impinges on the effectiveness of the Article 46 GDPR transfer tool the data exporter is relying on, or the data exporter intends to rely on in the context of the transfer.

5. The following action is to take any **formal procedural steps, which the adoption of the supplementary measures** the organization may require, depending on the Article 46 GDPR transfer tool used. These recommendations specify these formalities. One may need to consult the competent supervisory authorities on some of them.

6. The final step will be for data exporters to **re-evaluate at appropriate intervals the level of protection** afforded to the data transferred to third countries and to monitor if there have been or there will be any developments that may affect it. The principle of accountability requires continuous vigilance of the level of protection of personal data.

When in Doubt: Keep the Personal Data in the EU

When no other legal mechanisms apply, the GDPR provides in an exception possibility for transferring personal data to a third country, but only when certain conditions are fulfilled. Probably the most relevant one in the perspective of software, cloud computing and other IT-related services is, that this legal basis can only be used for data transfers that are “incidental” or “not repetitive”. The EDPB has stated earlier and very clearly that derogations of Article 49 GDPR must be interpreted restrictively, so that the exception does not become the rule. When using this route, the level of protection for individuals guaranteed by the GDPR should not be undermined. And always with explicit consent of the data subject to the proposed transfer of his data.

In reality it probably will not always be possible to take those additional measures that sufficiently protect personal data. Some countries simply do not sufficiently protect privacy and other fundamental rights.

Hidden Privacy Risks of Redundant Domain Names and Email Addresses

An “ethical hacker” in the Netherlands intercepted e-mail correspondence addressed to Dutch police officers over a period of one and a half years, starting mid-2015. He did this by registering old domain names that the police

used to use, and also registered domain names that are very similar to those of the police force. Before the introduction of the National Police, each force deployed its own domain name and therefore its own e-mail addresses. Nowadays, every employee has their own police.nl email address. If people use an old address, or accidentally have it in their contacts, things go wrong.

In another case, with the same cause but this time reported by a Dutch news outlet in April 2019, a major data breach occurred at the Utrecht Youth Services Agency. Well over three thousand case files and two hundred voicemails and internal mails containing full details of vulnerable children were compromised through the — careless — cancellation of a disused domain name when the organization renamed itself to SAVE. In the meantime SAVE learned five lessons from this practice:

- do not cancel a domain name immediately after switching;
- make an overview of the domain names and the purpose for which they are used;
- inform employees about no longer using domain names and email addresses;
- monitor malicious registrations and login attempts; and
- use multifactor authentication.

Drawing up an adequate management policy and carefully implementing it prevents the risk of data leaks.

Adjacent privacy risks

Organizations not only have to carefully manage current and redundant domain names, the same applies to corporate email addresses. Especially those of people leaving the company or public sector organization create a data privacy risk — and legal liabilities as well. In a recently published decision, the data protection authority of Belgium — Gegevensbeschermingsautoriteit (GBA) — has taken a practical position on the management of mailboxes of former staff. As a result, many organizations will have to rethink their processes.

The case investigated by the GBA involved a family business where the CEO was abruptly fired, and others followed suit. After which only their professional e-mail addresses remained in use. In the case of the CEO, this was still the case more than two and a half years after his departure. As a result, the former CEO demanded the discontinuation of these email addresses, with the GBA fining the company in question of Euro 15.000 on 29 September 2020. The data protection authority took into account that it was a relatively small company, with just over ten employees. The fine is based on the violation of the GDPR privacy principles of purpose limitation and data minimization (limitation of the conservation).

The GBA advises employers to block the mailbox of an employee — who has left his position — as soon as possible. In parallel, the organization must set up an automatic message so that all future senders are notified of the employee's departure for a reasonable period (usually one month). After this period, the mailbox will ideally be deleted.

Looking Ahead: Artificial Intelligence

The call for supervision of Artificial Intelligence (AI) and algorithms is growing in politics and society. Next to large companies (IBM, Google, Telefónica, Microsoft, SAP) and trade organizations (USACM, IEEE) parliaments (UK, France), the European Commission, and many other intuitions and partnerships have published code and principles for AI. And not without reason. On one hand use of algorithms offers many opportunities, and on the

other hand there are also serious risks involved. The main theme revolves around “human-centric” AI — and puts people first. In Europe, the data protection authorities are responsible for supervising the processing of personal data, and thus also for the application of AI and algorithms that use personal data.

The GDPR leads the way

If one considers all the codes and principles for AI, the temptation that artificial intelligence is moving in a legal vacuum arises. However, this thought does not rhyme with reality. AI and algorithms are also part of our society and are subject to legal rules for this reason alone. Every organization which deploys artificial intelligence technology is responsible for its use must know what the organization is doing and be transparent about it.

Looking at data privacy in junction with AI, in particular the general principles of lawfulness, fairness and transparency apply, as laid down in the GDPR. In concrete terms, this means that when using algorithms that process personal data, the following basic conditions must always be met:

- data processing needs a legal ground (for example, consent or the execution of a contract);
- data that is processed for one purpose, may not simply be used for another purpose at a later time (purpose limitation); and
- there are storage and security standards for the personal data, which depend on the nature of the personal data.

Another important criterion that applies in full to the use of AI when personal data is processed, is legal accountability. After all, the controller is obliged to keep a processing register in which activities in which personal data are processed are described, including the purposes of those processing operations. Furthermore, a controller must carry out an assessment of its effect on the protection of personal data prior to a particular processing. This so-called data protection impact assessment (DPIA) is usually mandatory when using algorithms. In this, a controller must substantiate why he or she uses certain data in an algorithm, what the purpose of the use of an algorithm is, but also why it is necessary to work with that algorithm. When these risks cannot be eliminated sufficiently, it is mandatory to submit a prior consultation to the competent data protection authority for advice.

Conclusion

Two and a half years after the GDPR became applicable (May 18, 2018), the specialized legal domain of data privacy law is in full swing. The nullification of a crucial agreement between the European Union and the United States (the Privacy Shield framework) created — again — uncertainty for transatlantic data transfer which the European Data Privacy Board tries to solve with its brand-new recommendations, leading case law on data breaches and other GDPR infringements in various EU member states was passed (to be addressed in the next briefing), hidden privacy risks are emerging from unexpected quarters, and, for example, the rise of advanced artificial intelligence (machine learning) and its consequences for the protection of privacy causes an inconvenient struggle between innovation and regulatory compliancy.

Furthermore, events related to COVID-19 control measures demonstrate the complexity of the lawful processing of health data in daily practice; whether or not related to the work place or the development (privacy by design) and use of contact and tracing apps. Moreover new profound legalisation is in sight, such as the upcoming ePrivacy Directive, which contains a tightened legal framework for the processing of personal data at electronic communications and for marking purposes, which forms an addition (lex specialis) to the GDPR.

Every organization must focus on the laws and regulations for the processing of personal data. Strategic-legal decision making and corporate polices, however, should address a wider range of digital law compliancy issues in conjunction with data privacy.

About Hitachi Vantara

Hitachi Vantara, a wholly owned subsidiary of Hitachi, Ltd., guides its customers from what's now to what's next by solving their digital challenges. Working alongside each customer, we apply our unmatched industrial and digital capabilities to their data and applications to benefit both business and society. More than 80% of the Fortune 100 trust Hitachi Vantara to help them develop new revenue streams, unlock competitive advantages, lower costs, enhance customer experiences, and deliver social and environmental value.
www.hitachivantara.com.

About Data Matters

Data Matters designs and delivers sustainable archiving solutions and services with an integrated management for paper-based archives and digital preservation, including a digital repository with all the functions defined in the OAIS model. These solutions and services are based on years of expertise, in-depth multi-disciplinary knowledge, and industry-leading products and services from select innovative and reliable technology manufacturers. Data Matters has long-standing partnerships with Hitachi Vantara, Star Storage, and others.
www.datamatters.nl

About the author

Victor Alexander de Pous is a senior corporate lawyer, analyst and strategist who has been working in the domain of the legal aspects of digital technology, electronic data processing and the information society since 1983. Selective Bibliography: http://thelegallook.nl/

Version: December 2020