DATA MATTERS

HITACHI
Inspire the Next

A New Technological Reality Forces the EU to Reinvent Key Legislation for the Confidentiality of Electronic Communications Content and Metadata of that Content

EXECUTIVE LEGAL BRIEFING SERIES

The Upcoming EU ePrivacy Regulation

Outdated Personal Data Processing Legislation for Electronic Communications Receives Major Update in Line With GDPR

By Victor Alexander de Pous
April 7, 2021

LEGAL BRIEFING #4: ePrivacy Law

Contents

LEGAL BRIEFING #4: ePrivacy Law

Headlines

- In their minds, many organizations probably have only just adjusted the internal and external business processes to the requirements of the General Data Protection Regulation (GDPR) — and must update the privacy and data policies and processes as we speak due to new developments (see Legal Briefing #3) — or a new, additional European data privacy law presents itself. The European Union is re-sharpening the conditions for business operations again, now for a high privacy level in the respect of electronic communications services.

- The upcoming ePrivacy Regulation, which will replace the 2002 ePrivacy Directive, means a thorough revision of the outdated existing regulatory framework. Essential to understand: while the GDPR covers all forms of personal data processing, the ePrivacy Regulation focusses specifically on the (i) processing of personal data and (ii) non-personal data (iii) in electronic communications services as such. From the confidentiality of e-mails and WhatsApp messages to the use metadata and HTTP cookies. It is once more considered key legislation for the digital space in Europe.

Analysis

- The underlying reason for new privacy and electronic communications rules is that EU legislation needs to keep up with the fast pace at which IT-based services are developing and evolving, which includes new players providing electronic communications services such as instant messaging apps (WhatsApp, Facebook Messenger, and Signal), VoIP platforms, and the machine to machine (M2M) transmitted over a public network.

- Next to the technological modernizing ground, serves the legal driver of truly harmonizing rules within the European bloc, eliminating national differences in interpretation of legislation and through case law. With the new privacy and electronic communications services law the European Commission chose for a *regulation* again. That means that the ePrivacy Regulation is self-executing and requires very little implementing measures in the national legislation of the 27 member states of the EU. Moreover, if national law contradicts an EU regulation, the regulation takes priority.

- Initially intended to enter into force simultaneously with the General Data Protection Regulation (GDPR) on 25 May 2018, the ePrivacy Regulation ran into substantial delays, especially due to fierce lobby practices from the market place. Only on 10 February 2021 and then after a tiresome negotiation process, the European Commission's Council — during the Portuguese Presidency — finally took a common position and anchored it in a newly adapted proposal on high level of privacy rules for *all* electronic communications.

- While the GDPR must be considered in legal terminology as the *Lex generalis*, the current ePrivacy Directive and the upcoming ePrivacy Regulation are *Lex specialis*. This means that (i) the ePrivacy law supplements the (general) rules on the protection of personal data of the GDPR, and (ii) that where the two legal frameworks conflict, the ePrivacy law prevails.

- The notorious political sentiment dominates at the moment of achieving the ePrivacy Regulation 2021 draft proposal of the EU Council. "Robust privacy rules are vital to create and maintain trust in the digital world," says the European Council. And: a good balance has been found between "solid protection of the private life of individuals and promoting the development of new technologies and innovation". Notably, this balancing act is a very difficult one — and the last thing about it has not been said yet.

- In its Statement of 3 March 2021, the European Data Protection Board (EDPB) sees room for improvement, after the 2021 draft proposal. The new law should (i) not reduce the level of protection of personal data for Europeans and (ii) at all times be *fully* aligned with the GDPR. “In no way the ePrivacy Regulation can be used to de facto change the GDPR.”

The Current EU Law on Privacy and Electronic Communications

In the 2015 digital internal market strategy, the European Commission announced a renewal of the Directive on Privacy and Electronic Communications, known as the ePrivacy Directive (2002/58/EC) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. At this time the law still regulates:

- **Confidentiality of communications**: EU Member States must ensure the confidentiality of communications over public networks, in particular by prohibiting the listening into, tapping and storage of communications without the consent of the users concerned.
- **Security of networks and services**: a provider of a public electronic communications service has to take appropriate measures to safeguard the security of its service.
- **Data breach notifications**: if a provider suffers a breach of security that leads to personal data being lost or stolen, it has to inform the national authority and, in certain cases, the subscriber or individual.
- **Traffic and location data**: this data must be erased or made anonymous when no longer required for communication or billing purposes, except if the subscriber has given consent for another use.
- **Spam**: subscribers must give their prior consent before unsolicited commercial communications ("spam") are addressed to them. This also covers SMS text messages and other electronic messages received on any fixed or mobile terminal.
- **Public directories**: subscribers' prior consent is required in order for their telephone numbers, e-mail addresses and postal addresses to appear in public directories.
- **Calling-line identification:** subscribers must be given the option not to have their telephone number disclosed when they make a call.

Directive

The current rules for privacy and electronic communications are laid down in a *directive*, which means that they had to be implemented in the national legislation of each of the 27 member states of the EU. As a consequence, sometimes even substantial differences in the various jurisdictions occurred in the legislation itself and furthermore through its interpretation by the courts of law. For example, the Netherlands changed the regulation for the use of cookies frequently, creating confusion in the marketplace.

A New Technological and Legal Reality

Important changes in electronic communications have taken place in recent years, which justify a revision of the ePrivacy Directive. Think of the large quantities of communication services based on the Internet. In addition, the GDPR entered into force on 25 May 2018. The Commission therefore wants to revise and adapt existing electronic privacy rules to the GDPR, and at the same time adjust the regulations to the digital challenges of the present legal age.

The European Commission held a public consultation from April to July 2016 on the ePrivacy Directive. The 421 responses showed that it is endorsed that many special privacy rules are required in the electronic communications sector; in particular to guarantee confidentiality. It turned out that the respondents found the scope of the ePrivacy Directive too low and the rules too vague, resulting in very different implementation by the various Member States in their national laws and regulations.

The original ePrivacy Regulation 2017 draft proposal of the Commission with a high level of privacy rules for all electronic communications includes a variety of starting points, which after all negotiations still exist. The rules must apply to new players providing electronic communications services and have the same level of confidentiality as traditional telecoms operators. Privacy will also be guaranteed for communications content and metadata, while metadata have a high privacy component and should be anonymised or deleted without the user's consent, unless the data is needed for billing.

Other basis relate to new business opportunities, simpler rules on HTTP cookies, protection against spam, and a more effective enforcement of the confidentiality rules by the national Data Protection Authorities (DPAs), already in charge of the rules under the GDPR. On 10 February 2021 and then only after a tiresome negotiation process, the European Commission's Council took a common position and anchored it in a newly adapted proposal.

Understanding the Concept of Lawful Processing of Personal Data

Understanding the lawfulness of personal data processing is crucial for any business and public sector organization. The main rule reads an organization may only process personal data as such when based on one or more of the six grounds exhaustively listed in Article 6 GDPR,. These grounds are as follows:

1. The data subject has given **consent** to the processing of his or her personal data for one or more specific purposes.
2. Processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
3. Processing is necessary for **compliance with a legal obligation** to which the controller is subject.
4. Processing is necessary in order to protect the **vital interests of the data subject** or of another natural person.
5. Processing is necessary for **the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
6. Processing is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Looking at the ePrivacy Regulation 2021 draft proposal of the EU Council, consent of data subject (basis #1) forms the major ground for processing his/her personal data in respect to electronic communications services, and additional the legitimate interests pursued by the controller or by a third party (#6). New is performance of a contract as a lawful ground for processing personal data. The other three bases do not comply.

Cookie Walls: Today and Tomorrow not Permitted

How relevant and far-reaching the data subject's given consent **to** the processing of his or her personal data for one or more specific purposes is, derives from the discussion on the use of so-called 'cookie walls". As known, a broad variety of HTTP cookies perform essential functions in today's Internet, existing of a small piece of data stored on the user's *terminal equipment* (PC, laptop, smartphone, smart car, smartwatch, et cetera) by the web browser while browsing a website.

Especially the use of tracking cookies, including third-party cookies raise privacy concerns. Often these are advertising cookies. Some website operators deny users access if they do not consent to all cookies and trackers present on that website. For placing tracking cookies, an organization must ask for prior permission, as the GDPR requires. This applies if an organization operates a website, but also with apps or other services. On 4 May 2020 the European Data Protection Board (EDPB) adopted guidelines for GDPR compliance that clarify what constitutes valid consent for personal data processing in the EU**,** while at the same time confirming that the use of Cookie Walls as a way of obtaining lawful consent is non-compliant**.**

Please note: the prohibition on Cookie Walls does not only relate to placing HTTP cookies, but also to comparable techniques for which consent must be requested. These are techniques such as JavaScript, flash cookies, html5-local storage and / or web beacons. The GDPR sets strict requirements for valid consent and stipulates in Article 4(11) that consent of the data subject means any:

- freely given,
- specific,
- informed, and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

According to the EDPB “the element ‘free’ implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if he/she does not consent, then consent will not be valid.” In the perspective of a Cookie Wall, the website visitor / user does not have a genuine or free choice. *The consent is not freely given*, because access to services and functionalities are conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in his terminal equipment.

Although the ePrivacy Regulation 2021 draft proposal raised concern at the EDPB on the subject-matter of the use of Cookie Walls, the independent European body stresses “the need to include an explicit provision in the ePrivacy Regulation to enshrine this prohibition, in order to enable users to accept or refuse profiling.”

More 2021 Draft Proposal Takeaways

The ePrivacy Regulation 2021 draft proposal of the EU Council under the Portuguese Presidency is divided in five chapters, which relate to (i) the material, subjective, and territorial scope of regulation, (ii) requirements and limitations for accessing data on end-users’ devices, (iii) requirements and limitations for number-based interpersonal communications services and direct marketing communications, (iv) identifies the authorities responsible for enforcing the regulation and their powers, and (v) describes remedies, liability and penalties.

In general, the directive regulates the confidentially of electronic communications, metadata, HTTP cookies and similar technology, unsolicited communication (spam), and direct mail. Any organization in any country will be subject to the ePrivacy Regulation (Article 2) when:

- processing electronic communications content and metadata of that contact of end-users who are in the European Union;

- processing terminal equipment information of end-users who are in the European Union;
- providing a publicly available directory of end-users of electronic communications services who are in the European Union;
- sending direct marketing communications to end-users who are in the European Union.

Some important amendments of earlier drafts of the regulation made include:

- Widening the territorial scope, which now also applies to the processing of personal data by a controller not established in the European Economic Area (EEA: EU member states + Iceland, Liechtenstein, and Norway), but established in a place where Member State law applies by virtue of public international law.
- Widening the material scope. "Processing" relates not only to personal data (as in the GDPR), but also to other data, that is non-personal data.
- Although "metadata" is covered in the current ePrivacy Directive, the new draft broadens the options for providers of electronic communications services to process metadata.
- Adding the definition of "location data" (a type of metadata): "data processed by means of an electronic communication network or service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".
- Widening the material scope: the "provisions for consent" — as one of the six bases of lawfulness of personal data processing of the GDPR — shall apply to natural persons and, *mutatis mutandis*, also to "legal persons".
- Inserting processing for the "performance of a contract" as another ground for the lawful of personal data processing.
- Requiring service providers sharing anonymized statistical electronic communications data with third parties to carry out a data protection impact assessment (PIA's) and inform end-users of the envisaged processing operations.

The fines of the ePrivacy Regulation will be similar to the regime of the GDPR: a maximum penalty of Euro 20 million or 4% of a non-compliant organization's global annual revenue, whichever is higher.

Strong Position of the European Data Privacy Board

While the EDPB welcomes the Council's position as a positive step towards a new ePrivacy Regulation; the Board makes it also very clear that: "In no way the ePrivacy Regulation can be used to de facto change the GDPR". This means that under no circumstances the level of protection offered by the current ePrivacy Directive may be lowered, but should complement the GDPR by providing additional strong guarantees for confidentiality and protection of all types of electronic communication.

Next to the need for an explicit provision on Cookie Walls, the EDPB proposes a number of changes. Other important issues are:

- Data from confidential electronic communication, such as WhatsApp messages, text messages and e-mails may only be used for *necessary goals* without permission. For example, ensuring that a message ends up with the recipient and guarantee a secure connection. This also applies to metadata, such as location data, which will be included in a message.

- The supervision of the use of personal data within the ePrivacy Regulation should completely be exercised by the same supervisors of the GDPR, which means the data protection authorities of the EU member states. Dissemination of supervision is not permitted.

- Although the discussion about access to encrypted data and communication by law enforcement agencies comes up time after time, end-to-end encryption — from the sender to the recipient — is the only way to ensure full protection of data in transit. “Any possible attempt to weaken encryption, even for purposes such as national security would completely devoid those protection mechanisms due to their possible unlawful use. Encryption must remain standardized, strong and efficient.”

Especially these issues will be addressed in the upcoming negotiations. Both the EU Council and the EDPB clearly indicate the necessity for alignment of the ePrivacy Directive with the GDPR, but work-out this principle somewhat differently. The EDPB seems notably stricter. A Lex specialis may derive from a Lex generalis indeed; however, only by supplementing and not undermining the standard level of protection of the general law.

Conclusion

The proposal for the ePrivacy Regulation is the culmination of the European Commission's efforts to complete the data protection framework in Europe. The starting point is that the content of these messages is only accessible to the parties directly involved in the communication.

The intended one — high — level of protection for all electronic communications services and one single set of rules across the EU will probably be finalized the end of 2021. Compared to previous 13 proposals, the current ePrivacy Regulation 2021 draft proposal of the EU Council (i) simplifies the text of the law and (ii) provides one more in alignment with the GDPR. Both EU laws address personal data processing, but where the GDPR regulates all types of personal data processing, the ePrivacy Regulation will complement the GDPR with harmonized rules for electronic communications.

In comparison to the still applicable ePrivacy Directive framework of 2002, the upcoming ePrivacy Regulation will have a broader scope, incorporating (all) new technologies such as WhatsApp, Facebook Messenger and Signal (instant messaging), Skype cum sui (VoiP platforms) and machine-to-machine communications transmitted over a public network, including hardware and software deployments for the Internet of Things (IoT). Moreover, it aims to regulate both personal data and non-personal data in electronic communications services.

In other words, we are looking at a broader scope for important digital rules, which are also applicable to every public sector and non-profit organization.

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: April 7, 2021