WHITE PAPER

E-Privacy Unveiled: Decoding the Regulatory Realm of ePR

DPO Consultancy
Experts in Data Privacy

MAY 2024

Johan Martens
Deniz Naz Kaya

E-Privacy Unveiled: Decoding the Regulatory Realm of ePR

Introduction

2002 was the year that Euro coins and banknotes went into circulation. It was two years before the launch of Facebook, and three years before the first video was published on YouTube. Considering the substantial technological changes since the inception of the e-Privacy Directive (ePD) in 2002, the need for comprehensive and adaptive legislation was more pressing than ever in this era. The current directive primarily concentrates on safeguarding personal data, whereas the proposed e-Privacy Regulation (ePR), also known as the "Regulation concerning the respect for private life and the protection of personal data in electronic communications" seeks to replace the existing directive.

The content of electronic communications is the foundation of today's digital services. Calendars that sync meetings, applications that provide spellchecks for emails, and anti-spam filters for Internet browsers, these new technologies are all in need of electronic telecommunication data to be able to function. ePR aims to ensure that the confidentiality of electronic communications can be still protected without compromising either the advantages of new technologies or people's privacy.

The ePR serves a dual purpose. Firstly, it aims at protecting the electronic communications of legal persons. Secondly, establishing an internal market for electronic communications and ensuring its proper functioning are targeted. The latter promotes the need for European Union (EU) action in the context of the digital single market (DSM) strategy. The DSM strategy refers to the EU's initiative to create a single digital market, breaking down barriers and fostering a more integrated digital economy across member states.

I. Background

Although the first draft of the ePR was presented by the EU Commission in January 2017, it has been delayed in the approval process, pushing back its implementation. The ePR was set to come into force alongside the General Data Protection Regulation (GDPR) on May 25, 2018. Since then there have been 13 different drafts of the ePR. The ePR will replace the ePD and specify the GDPR for particular subjects concerning electronic telecommunication data.

The ePD came out in 2002, was revised in 2009, and in 2017, the EU Commission introduced the ePR. However, ePR's enforcement was delayed. Fast forward to 2021, the EU Council published a working draft for ePR after going through trialogues. Now, ePR is expected to be enforced around late 2024, bringing in some important changes to how electronic privacy is handled in the EU.

II. Scope

Material Scope

ePR has a broader scope than the ePD because of the extension of focus beyond traditional telecommunication services. "Electronic communications content," encompassing texts, voice messages, videos, and images, and "electronic communications metadata," which involves data used to trace the source and destination of the communication are the focus of ePR. It covers over-the-top (OTT) services like

WhatsApp and Skype; email services and machine-to-machine transmissions (Internet of Things (IoT) devices). ePR's applicability to legal entities widens its scope even beyond the GDPR, which exclusively addresses the personal data of natural persons. It is also applicable to information relating to end-user equipment (commonly referred to as cookies), the management of publicly accessible directories of users of electronic communications, and the transmission of direct marketing to end-users using electronic communications.

Article 2 of the ePR specifically outlines that the ePR does not cover:

- Activities beyond the scope of Union law.
- Activities of Member States falling under Chapter 2 of Title V of the Treaty on EU.
- Electronic communications services that are not publicly available.
- Activities of competent authorities related to preventing, investigating, detecting, or prosecuting criminal offenses, including ensuring public security.

Territorial Scope

ePR does not solely apply to the parties established within the EU, instead, it applies to the parties which are established outside the EU where member state law applies by public international law.

The location of the end-user plays a vital role in determining the scope. Specifically, it applies to end-users within the EU who receive electronic communication services, have their electronic communication content and metadata processed, or are recipients of direct marketing communications. In these cases where the involved parties are situated outside the EU and are exempted from the member state law by public international law, they are required to appoint a representative within the EU within one month of commencing their activities. However, this obligation is not applicable if only a small portion of the activities of the party falls under the ePR or the activities are unlikely to cause a risk to the end users concerning their fundamental rights.

IV. Enforcement

National data protection authorities (DPAs) within the EU are responsible for the enforcement of ePR. They are primarily the same bodies who are responsible for the enforcement of the GDPR. Each EU member state has a designated DPA, that monitors the proper application of data protection. These authorities have the power to investigate complaints, issue fines and conduct audits. The European Data Protection Board (EDPB) coordinates these authorities to ensure consistency across Europe.

The "one-stop shop" mechanism outlined in GDPR applies to the enforcement of ePR as well. In other words, organizations that operate in multiple EU states deal primarily with the DPA in the member states where they have their main EU establishment. However, all relevant DPAs can be involved where there is a case of cross-border implications.

V. Obligations

Confidentiality of Electronic Communications Data

Confidentiality is essential in online conversations. This is the reason why ePR aims to make the content of emails, instant messages, or even smart-home devices as private as a conversation in the individual's living room. However, there are some exceptions.

Service providers might feel the need to interfere with the content of the messages and calls to ensure they reach their intended destinations. From time to time, a security breach or a glitch is inevitable, especially for bigger service providers. Postal workers scanning the address on the envelope to make sure the envelopes reach their destination might be an example of this exception.

Consequently, the first exception applies to the cases where:

- The interference is necessary for transmitting the communication, for the duration required or
- It is necessary to maintain or restore the security of electronic communications networks and services, or
- To detect technical faults and errors in transmission, for the necessary duration.

Suspicious activities are often encountered such as someone trying to use another person's subscription, or suddenly the speed of the internet may fall. If an individual gives the consent for access to the location data for tracking purposes, such as for a fitness application, providers are allowed to use the data to track the runs. Such events require an exception due to investigation reasons. Therefore; electronic communications service providers may process electronic communications metadata if;

- It is necessary to meet mandatory quality of service requirements or
- It is necessary for billing, calculating interconnection payments, or detecting and stopping fraudulent or abusive use of, or subscription to, electronic communications services or
- The end-user has given consent for processing their communications metadata for specified purposes, including providing specific services, as long as the purpose cannot be achieved by processing anonymous information.

The last exception to confidentiality appears when service providers process electronic communications content only;

- For the sole purpose of providing a specific service to an end-user, with the end-users consent, if the service cannot be provided without processing such content or
- If all end-users involved have given their consent for processing their electronic communications content for specific purposes that cannot be achieved by processing anonymous information. The provider must consult the supervisory authority, following the procedures outlined in Article 36 of GDPR.

Storage and erasure of electronic communications data is in line with GDPR, meaning that the service providers must erase or make anonymous the content after it has been received unless otherwise authorized by the end-user. For the metadata, providers of electronic communication services must erase or make anonymous when it is no longer needed to transmit the communication unless the metadata is processed for billing purposes, in which the providers may keep the data until the end of the period during which the bill may be challenged.

Cookies

ePD was the first legislation to specify the rules for the use of cookies on websites, which are used to process user data. A notable requirement brought by ePD was the cookie banners, which are designed to obtain consent concerning the collection of their data during their first visit to the website. Similarly, GDPR also mandates websites to obtain specific consent.

ePR also maintains the requirement to obtain consent prior to the installation or use of cookies, except when cookies are necessary for providing electronic communication services. Article 8 of the ePR forbids using cookies in general, with several exceptions, such as when cookies are required to provide an electronic communication service, to provide a service that the end-user has specifically requested, or for the exclusive purpose of audience measuring.

Before processing any form of data from users' computers or smartphones, ePD requires obtaining the end-user's consent. The ePR, on the other hand, addresses cookie consent fatigue—a condition in which users become exhausted of providing consent on websites all across the Internet—and offers new methods to simplify consent across browsers, including the option to express consent through browser settings.

ePR also specifies that cookie walls, linking website access to user consent for cookies, may not be permissible for dominant service providers or public authorities. Conditioning access is only acceptable when an alternative option without cookie consent is provided, ensuring a genuine choice for the user. Although obtaining user authorization to visit a website is typically appropriate, there are several exceptions, particularly for public authorities or dominant service providers, or in situations where there is an obvious imbalance between the end-user and the service provider. For example, a government website or a major social media platform cannot block access to their services unless the user consents to tracking cookies. Instead, they should offer an alternative, such as the option to subscribe for a fee as an alternative to accepting cookies for personalized advertisements.

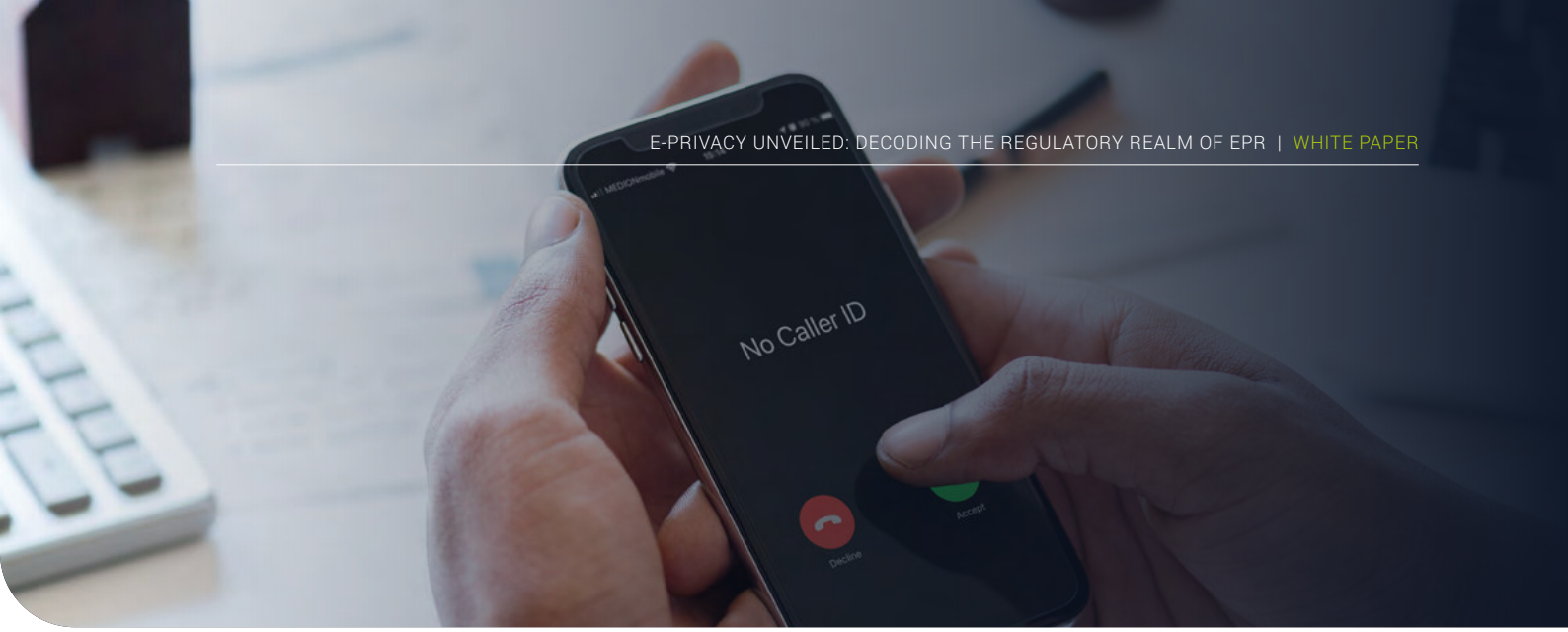
ePR broadens exceptions to user consent requirements to include audience-measuring cookies, security-related cookies, and cookies necessary for software updates. Users have the flexibility to grant consent to specific types of cookies by whitelisting providers in their browser settings, with the ability to modify these whitelists and withdraw consent easily. This simply provides the freedom to consent to specific types of cookies.

Rules on the use of cookies will be stricter, compared to the ePD. Consent is required when cookies are used for advertising purposes or personalizing a website, for instance. Cookie walls, which prevent access to a website unless a user agrees to the use of cookies, should only be used in situations where website visitors are given a genuine, free option to choose between services based on accurate, clear, and user-friendly information (e.g., choosing between accessing website content in exchange for payment or consenting to the use of cookies). Pre-ticked boxes, which require users to untick boxes to remove optional cookies, should be avoided.

ePR introduces a new rule as well. Software used for electronic communications, including browsing the internet, must provide an option for end-users to prevent third parties from storing information on their devices or processing information already stored. In simpler terms, software used for electronic communications should allow users to control how their information is stored and processed. Users must be notified about privacy settings during installation, and software that was created before May 25, 2018, must comply with these privacy settings at the time of the first update, but no later than that date.

Presentation and Restriction of Calling and Connected Line Identification

Article 12 of ePR regulates the privacy and the control that individuals have over their telephone numbers and the related identification information when making or receiving telephone calls. Users can choose to restrict which outgoing calls show their phone number—a feature known as “caller ID blocking” or “Call Line Identification Restriction (CLIR)”—or not. Furthermore, individuals have the option to hide their phone numbers both during and after the call. This may be achieved by selecting the “call without disturbance” preset. For incoming calls, individuals have the right to block calls from those who have hidden their numbers. Moreover, they can choose to prevent their number from being revealed during a conversation. Service providers are required to offer these functionalities at no additional cost and with simplicity of use.



Exceptions to these rules are outlined in Article 13 of the ePR. Notably, calls made to emergency services will have the caller's number revealed, regardless of blocking preferences. Additionally, in the case of persistent harmful or annoying calls, individuals can request their service provider to temporarily disclose the caller's number.

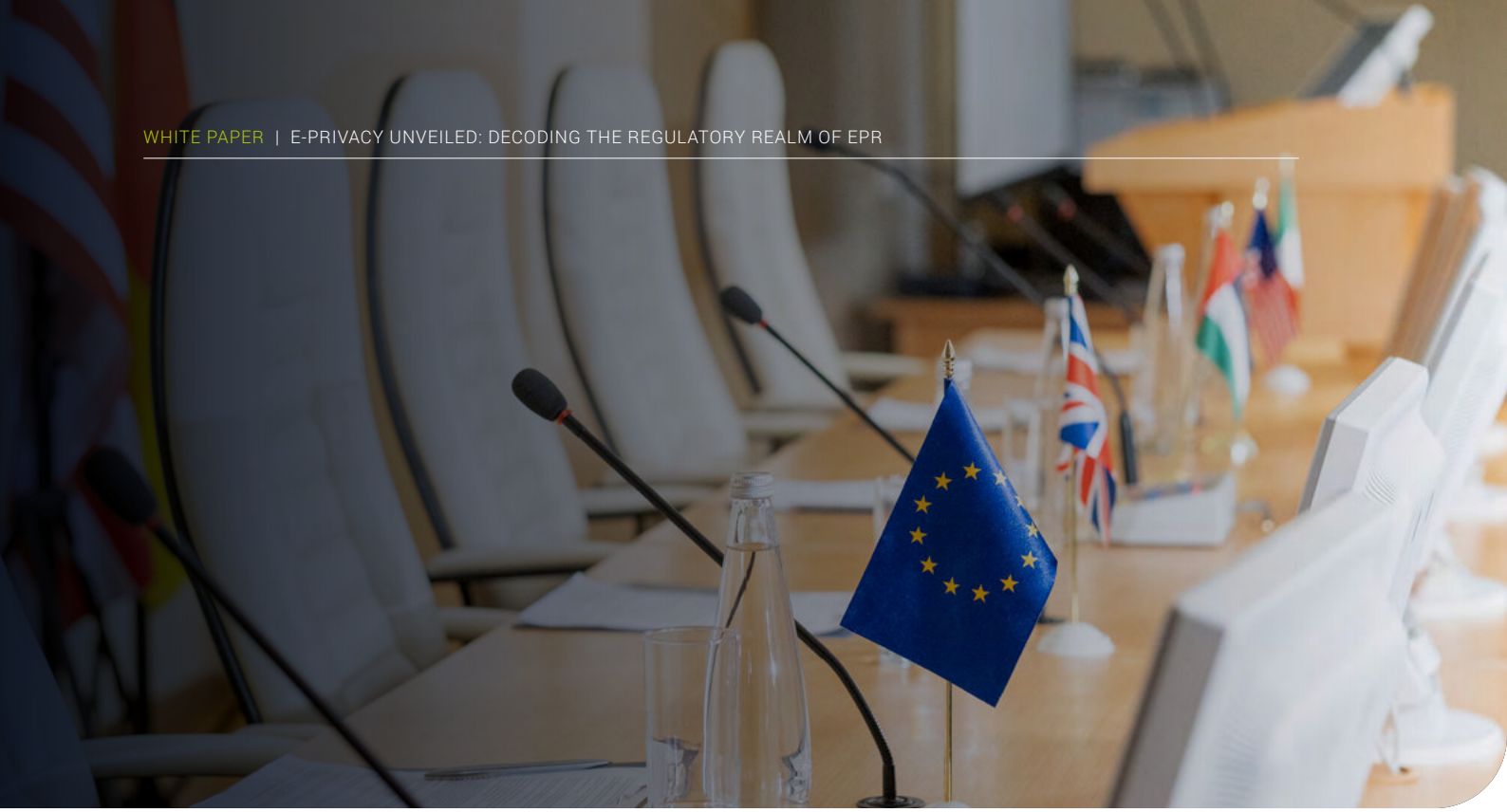
Unsolicited Communications

Concerning unsolicited communications, ePR aims to protect individuals from unwanted marketing, sent without the prior consent of the recipient. As a rule, consent is required upon receiving any direct marketing messages via electronic communication services. The exception to this rule appears when an individual is already a customer of the company. In this case, the contact details of the individual can be used to market similar products or services. Even with this exception, the company must provide a clear option to object to any kind of marketing.

Specific guidelines are also in place for marketing calls. Callers are required to either display their phone number or use a designated code or prefix that identifies the call as marketing-related. ePR extends to protect both individual consumers and business or legal entities.

VI. Non-Compliance

Mirroring the rights under the GDPR, there can be serious consequences for noncompliance with ePR. If their ePR rights are violated, end users have the right to pursue a judicial remedy. This aligns with Articles 77, 78, and 79 of the GDPR, which allows for complaints to supervisory authorities and the right to an effective judicial remedy against a supervisory authority or a data processor or controller. Legal actions may be taken by any person or entity that is harmed by a violation of the ePR, including competitors, in addition to end users. This includes providers of electronic communications services, who may have a stake in preventing violations that have an impact on their company.



End-users who suffer material or non-material damage due to an infringement have the right to compensation from the infringer unless the infringer can prove they weren't responsible for the damage. Violations relating to communication secrecy, consent for the processing of electronic communications data, and specific responsibilities of natural or legal entities can lead to fines of up to €20 million, or 4% of the global annual turnover, whichever is higher. Penalties for other designated violations may reach a maximum of €10 million, which is equivalent to 2% of the global annual revenue.

Each Member State is responsible for setting rules on penalties for infringements of the ePR not covered by Article 23's administrative fines. Member States are required to notify the Commission of these regulations, and the sanctions must be appropriate, effective, and deterrent.

VII. How Does the e-Privacy Regulation Differ from the GDPR?

Both GDPR and ePR address the same issue of protecting personal data within the EU, yet they focus on the different aspects of privacy, concerning different scopes of application. The GDPR aims to protect the rights and freedom of individuals by regulating the processing of personal data of individuals within the EU territory. In contrast, the ePR is designed to protect the confidentiality of electronic communications. This means the GDPR is comprehensive in its coverage, regulating the processing of personal data across a multitude of sectors. On the other hand, the ePR focuses on the specific area of electronic communications privacy.

The GDPR enforces significant penalties whereas the ePR is set to implement fines, establishing itself as lex specialis. Since ePR focuses on up-to-date communications such as instant messaging and Voice over Internet Protocol (VoIP) services, this feature is particularly important given that the ePR takes precedence in instances where the GDPR outlines a more general principle.

Another difference appears in terms of scope, where the GDPR applies only to the organizations that collect and process personal data of individuals within the EU and the ePR is applicable to organizations that provide an electronic communications service, service over an electronic communications network, services or networks that are publicly available, and services and network in the EU.

The GDPR focuses on personal data collected from individuals or other sources that can identify an individual within the EU, either directly or indirectly. Conversely, the ePR covers the same as GDPR, but also includes personal data collected via "publicly available electronic communication" service or network and additionally applies to non-personal data.

When it comes to cookie walls, the GDPR does not allow them, whereas the ePR permits cookie walls if a cookie-less alternative is provided. Lastly, for analytics cookies, the GDPR does not have an explicit condition and allows them with consent, while the ePR allows cookies used for audience measurement without consent.

VIII. How Does the e-Privacy Regulation Differ from the e-Privacy Directive?

The ePR represents a significant evolution from the ePD. The main differences are particularly the scope and the legal impact. ePR extends beyond traditional telecommunication providers, encompassing all electronic communications services, including OTT services, thereby adapting to the modern digital marketplace. It also broadens the protection of confidentiality to include contemporary communication platforms such as instant messaging and email services.

In terms of legislative effect, the ePD required individual transposition into the legal framework of each EU member state, leading to a diversity of national implementations. In contrast, the ePR is designed to be directly enforceable, ensuring a consistent application of privacy standards across the EU. This harmonization aligns with the GDPR, standardizing penalties and reinforcing the EU's commitment to data protection.

Significant amendments under the ePR address the use of cookies, specifically the approach to user consent. While the ePD introduced the requirement for user consent for cookies, often resulting in consent banners, the ePR seeks to streamline this process. It aims to diminish the need for repetitive consent banners for non-intrusive cookies, proposing a more centralized consent framework.

Additionally, the ePR builds upon the ePD's provisions concerning marketing communications. While the ePD requires prior consent for unsolicited communications, the ePR upholds these requirements and provides more explicit guidance, particularly regarding the exceptions to the rule.

IX. Conclusion

The evolution from the ePD to the ePR is a significant step forward in the protection of personal data and the private lives of individuals within the realm of electronic communications. The proposed regulation, with its meticulous organization into five coherent chapters, promises a more robust and clearer legal framework that addresses contemporary challenges brought about by technological advancements and the increasing digitalization of communication.

As the ePR replaces the outdated directive, it maintains the EU's dedication to ensuring that privacy and data protection are not just values but enforceable rights. The ePR offers clarity, security, and trust for individuals and businesses, fostering a digital ecosystem where privacy is integrated by design and respected in practice.

Bibliography

- Clifford Chance. (2022, February). E-privacy check-in – where we are – and where we're headed. Talking Tech. Retrieved from https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/02/e-privacy-check-in--where-we-are--and-where-we-re-headed.html

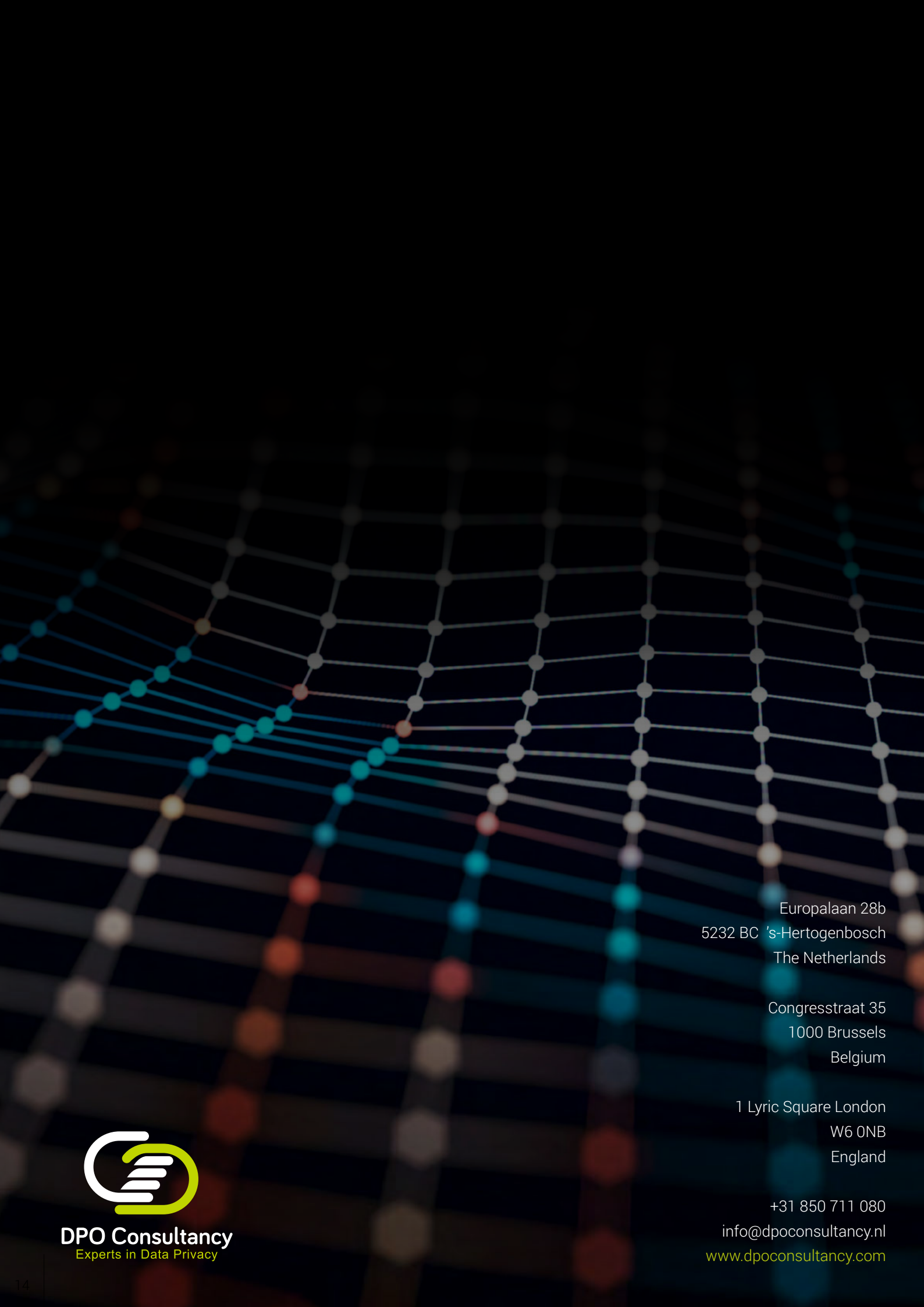
- CookieYes. ePrivacy Regulation. Retrieved from https://www.cookieyes.com/blog/eprivacy-regulation/

- European E-privacy Regulation. Retrieved from https://www.european-eprivacy-regulation.com/

- Michalsons. ePrivacy Regulation – Privacy Electronic Communications (PECR). Retrieved from https://www.michalsons.com/focus-areas/privacy-and-data-protection/eprivacy-regulation-privacy-electronic-communications-pecr

- The EDPB's Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC) – wp247

- Turing Law. The e-Privacy Regulation: Will it come after all? Retrieved from https://www.turing.law/the-e-privacy-regulation-will-it-come-after-all/



Europalaan 28b
5232 BC 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

1 Lyric Square London
W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com

DPO Consultancy
Experts in Data Privacy