www.pwc.ch/

Is ePrivacy defining the future standard of data protection for the banking industry?

The ePrivacy Regulation (ePR) and its impact on banks

"The question of the right to privacy must be one of the defining issues of our time."

S. Shetty

pwc

Table of Contents

The ePrivacy Regulation (ePR) and its impact on banks

The European Commission is finalising the ePrivacy Regulation (ePR), which may become effective, together with the EU GDPR, from May 2018. The ePR, which protects the right to respect for private life and communications, is one of the key pillars of the EU's Digital Single Market Strategy.

This new regulation is designed to be 'future-proof': all existing and future communication technologies are and will be subject to it. This will have a disruptive effect on banks' digital strategies, which will have to be redefined in line with the new requirements.

The ePrivacy Regulation in a nutshell

The ePrivacy Regulation will replace the existing ePrivacy Directive, which was revised in 2009. The new regulation comprises several adjustments to address current trends in digital markets and it entails a considerable extension of scope. The key goal of the ePrivacy Regulation is to protect electronic communications of natural and legal persons and to protect the information stored in their terminal equipment.

Legal background

In the recent years, electronic communications services have evolved significantly. Consumers and businesses are relying more and more on internet-based services to communicate, such as instant messaging, Voice over IP and web-based e-mail, which are not covered by the current ePrivacy Directive. The proposed Regulation on Privacy and Electronic Communications aims at reinforcing trust and security in the Digital Single Market. The draft regulation also aligns the rules for electronic communications services with the new world-class standards of the EU's General Data Protection Regulation (GDPR).

The cornerstones of the proposed rules on Privacy and Electronic Communications are:

- **All electronic communications must be confidential**
  Listening to, tapping, intercepting, scanning and storing of, for example, text messages, e-mails or voice calls will not be allowed without the consent of the user. The newly introduced principle of confidentiality of electronic communications will apply to current and future means of communication - including, for example, all appliances linked to the IoT ('Internet of Things').

- **Confidentiality of users' online behaviour and devices has to be guaranteed**
  Consent is required to access information on a user's device – the so-called terminal equipment. Users also need to agree to websites using cookies or other technologies to access information stored on their computers or to track their online behaviour.

- **Processing of communications content and metadata is conditional on consent**
  Privacy is guaranteed for the content of communication as well as metadata – for example, who was called, the timing, location and duration of the call, as well as any websites visited.

- **Spam and direct marketing communications require prior consent**
  Regardless of the technology used (e.g. automated calling machines, SMS or e-mail), users must give their consent before unsolicited commercial communications can be addressed to them. Marketing callers will need to display their phone number or use a special prefix number that indicates a marketing call.

Key requirements of the ePrivacy Regulation

The ePR has an extensive material scope as it includes rules on various aspects of electronic communications. The following are the key requirements outlined in the draft regulation.

- **Scope: legal and natural persons in the EU**
  The regulation applies to both legal and natural persons and covers the provision of e-communication services and the use of such services by such users within the Union. The regulation additionally applies to information related to the terminal equipment of users within the Union.

- **Protection of electronic communication**
  Electronic communication is protected through the principle of confidentiality. Accordingly, the processing of data and metadata related to electronic communications is restricted to what is strictly necessary to provide the communication service and erasure is required once the data is no longer needed for its original purpose. This will impact, for example, Voice over IP and instant messaging services (e.g. WhatsApp, Facebook messenger, Gmail, Skype).

- **Protection of information stored in terminal equipment**
  The regulation restricts the processing of data stored in the terminal equipment of users as well as the collection of information related to the user's terminal equipment.

- **Privacy settings**
  Protection of privacy will be strengthened through extended requirements relating to the consent to cookies, such as the need to provide transparent information on privacy settings and to offer possibilities to change privacy settings for all third-party cookies (via the browser settings). According to the current draft, the browser settings will need to allow website visitors to accept or refuse cookies from all websites, as well as other 'identifiers' – which is a change from the current cookie 'popups' that users see on most websites today.

- **Extended requirement for user's consent**
  The ePR will require the user's consent in a number of instances, for example, for the processing of e-communication content and related metadata (when such processing is not strictly necessary for the provision of the service) as well as for using information stored in terminal equipment.

- **Right of natural and legal persons to control electronic communications**
  The regulation adds restrictions with respect to calling-line identification and strengthens the provisions for call blocking.

- **Restrictions on unsolicited communications**
  Privacy is further strengthened through extended consent requirements with respect to entries in public directories and unsolicited communications (via e-mail, calls or any other electronic service).

- **Transparency on security risk**
  Providers of electronic communication services have to inform users about the particular risks related to the security of networks and electronic communications.

The ePrivacy Regulation and the GDPR

The ePR aims at complementing and specifying the requirements set out under the EU GDPR, i.e. the EU General Data Protection Regulation, which will be applicable from May 2018. Since the two regulations may have points of overlap, it is important to notice that the rulings under ePR are *lex specialis* to the GDPR and therefore they will prevail over the GDPR's requirements in case of conflict (provided they do not lower the level of protection enjoyed by natural persons under the GDPR).

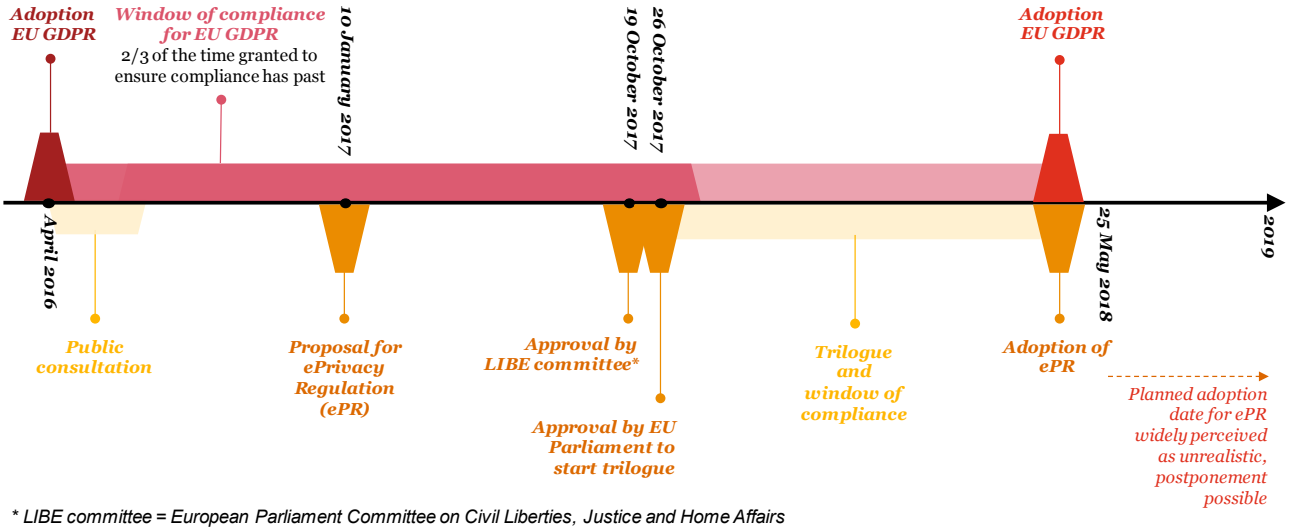
In light of the above, the following considerations are vital to the efficient and successful analysis and implementation of the two regulations.

Shared backbone

Due to their complementary nature, the two regulations share a number of similarities, most notably their national transposition model: both GDPR and ePrivacy replace existing directives. This means that they will be directly applicable without the need to be transposed into national laws and, as such, the playing field for the protection of electronic communications will be levelled across the EU.

Furthermore, the two regulations share the same enforcement model: the same supervisory authorities will oversee the application of the requirements and, in both cases, non-compliance may result in fines up to 4% of revenues or EUR 20 million, whichever is higher.

Finally, if the trilogue consisting of the European Parliament, the Council and the Commission, finishes the consultations in time, both regulations will be applicable as of May 2018.



* LIBE committee = European Parliament Committee on Civil Liberties, Justice and Home Affairs

Extended scope of ePR

While the GDPR focuses on protecting the personal data of data subjects within the Union, the ePR has an extended scope, as shown in the table below:

Scope	GDPR	ePrivacy	Scope extension by ePR
Data subjects	Natural persons	Natural and legal persons	Applies also to legal persons
Material scope	Processing of personal data	Processing of electronic communications data and information related to terminal equipment	Extension to any kind of electronic communication and information – not only personal data
Territorial Scope	• Controllers located in the Union • Personal data of subjects in the Union	Electronic services provided to users in Union (location at which the user uses the service)	Widening of territorial scope to use of electronic communication services in the Union

Extended scope of ePR

While the GDPR focuses on protecting personal data of data subjects within the Union, the ePR has an extended scope, as shown in the table below:

Scope	GDPR	ePrivacy
Protected data	Personal data	Metadata and information stored in terminal equipment
Principles	1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimisation 4. Data accuracy 5. Storage limitation 6. Integrity and confidentiality 7. Data protection by design and by default	Confidentiality of communication
Data subject rights	Rights created by GDPR: • right of access to personal data • right to rectification of inaccurate personal data • right to erasure • right to restriction of processing • right to data portability • right to object to processing • right to withdraw consent	Rights protected by ePR: • right of everyone to the respect of his or her private and family life, home and communications • rights to privacy and confidentiality of communications Rights created by ePR: • right to control electronic communications (including right to object to unsolicited communications)
Lawful ground	Lawful grounds for processing: • consent • necessary for contract performance • necessary for compliance • necessary due to public interest • necessary due to legitimate interests of controllers/third parties Under GDPR, there is now less need to request consent for the processing of personal data, as other lawful grounds are admissible	Consent is required for processing any kind of data, when the processing goes beyond what is strictly requested to provide the service (e.g. processing permitted without consent if it is required to perform communication transmission)
Data erasure	Data shall be deleted when no longer necessary	Certain data (e.g. content of communication) shall be deleted immediately; other (e.g. metadata for billing) to be kept no longer than necessary
Applicability outside of the Union (including Switzerland)	Applicable to non-EEA entities if they provide goods or services to data subjects domiciled in the Union.	Applicable virtually to any entity with a website or an app, unless access to them is restricted for users within the Union (i.e. if your clients can access your website from an EEA country, then your entity must comply to the ePR)

How does the ePrivacy Regulation affect you?

A number of banks have extensive programmes aimed at designing adequate processes to comply with the upcoming GDPR requirements. Compliance with GDPR will be the starting point; however, extra effort will be required to meet the additional rules set up in the ePR.

Key challenges of ePR for banks

Since the scope of ePR has increased compared with the GDPR, to ensure compliance, banks will have to expand the analysis of existing processes they had to complete in relation to the GDPR to all processes involving any kind of electronic communication with their clients, employees and any other type of data subject. The GDPR, in fact, was limited to the protection of personal data, while under the ePR the entire content of any electronic communication shall be protected. The key challenges arising from this increased scope and from the ePR as a whole are listed below.

- **Protection of legal persons**
  In the exercise of their day-to-day business, banks exchange a considerable volume of electronic communications (e.g. mails and voice calls) with their clients (natural and legal persons). Under the ePR, all these communications will be subject to stricter requirements, especially when they contain personal or confidential data, and this will translate into additional measures to ensure the protection of such data.

- **Protection of electronic communication**
  The ePR aims to protect all kinds of data processing within electronic communications. Banks may therefore have to develop new security requirements for the transmission of personal and confidential data through electronic means. This may affect existing processes such as fund transfers (where the data of the payer and payee is transferred between banks) or information exchanges related to regulations such as AEI (Automatic Exchange of Information), FATCA (Foreign Account Tax Compliance Act) or MIFID (Markets in Financial Instruments Directive). Most notably, this will affect e-mail communications.

- **Protection of terminal equipment information**
  The ePR covers not only the provision and use of electronic communication services but also the protection of information related to the terminal equipment of end users. Banks will have to consider these requirements, for example, in relation to their applications (such as e-banking apps) where data such as transaction details are stored by the user.

- **Future-proof requirements**
  The regulator is making sure that the definition of electronic communications in the ePR is broad enough to cover any possible technology – existing or future – used for electronic communication. In this sense, the ePR covers not only traditional communication services, such as e-mails and voice calls, but also all the 'Over-the-Top' (OTT) services that have proliferated in recent years and will continue to grow in the future (e.g. WhatsApp, Facebook, etc.), as well as any communications linked to the IoT. Banks started some years ago to build activities around OTT services (e.g. in certain cases, help desks can be contacted via social networks). Any ePR programme would have to review thoroughly the security measures and data processing purposes in relation to such activities.

- **Metadata restrictions**
  The restrictions relating to the processing and/or storage of metadata may affect the ability to use and analyse such data obtained from monitoring the use of bank websites or applications.

- **New regulations on cookies**
  The ePR aims at simplifying the user experience with cookies by allowing the user to set a global requirement for cookies directly in the browser; hence, it will be easier to block all third-party cookies. This may affect banks, as the effectiveness of targeted online advertisements (including in-app ads) will be limited under the new set-up.

- **Restrictions on unsolicited communications**
  Stricter consent requirements (with an 'opt-in clause') will limit the ability to access directly new potential clients using electronic means, including e-mails and voice calls. This may limit the possibility to generate new business – even in cases when contact details are collected from public directories. Similarly, HR departments may be restricted in their activities to contact a potential candidate.

- **Effects on internal screenings**
  As the processing of electronic communications will be prohibited without prior consent, internal screenings of e-mails (which is currently standard practice in the banking industry) will require prior consent by the employees and, potentially, by any user communicating with the bank. This would require banks to review thoroughly their current screening practices.

What is our suggested approach

The ePR is expected to come into effect by May 2018. Although the final regulation has yet to be published, banks could start assessing their readiness in relation to the draft regulation, as this would position them well when the final text is published.

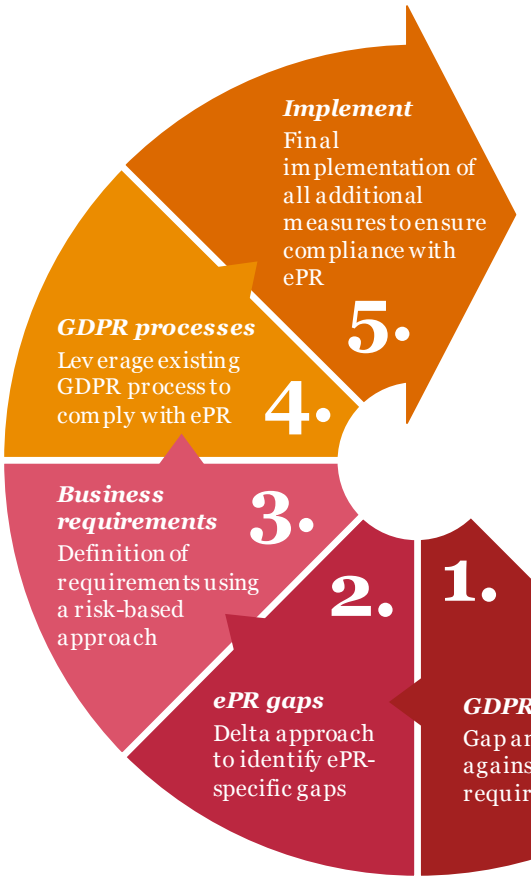
Prioritisation is key

In order to ensure an adequate prioritisation exercise, it is important first to understand how the ePR affects your bank. Which of the requirements are applicable and which are not? Which entities would be affected? Which systems and which processes? Clearly defining the scope of applicability of the ePR to your bank will be the first important step toward compliance, as the impact of the regulation will be very different depending on how much you rely on electronic communications and new technologies within your processes.

An ePR compliance programme cannot subsist without a comprehensive programme to respond to the GDPR's requirements (for companies that are subject to both regulations). The starting point to assess your readiness for the new regulation should be a gap analysis conducted in relation to GDPR. This will provide valuable insights on where your bank stands in relation to data protection. An additional analysis should then be performed using a delta approach, i.e. focusing only on the additional requirements of ePR that affect the banking industry.

The next steps will be to design and implement a compliance strategy that leverages as much as possible the ongoing programmes and measures for compliance with the GDPR. A holistic approach will ensure the consistency of your regulatory response and increase the efficiency of change management.

Like the GDPR programmes, you may have to consider a risk-based approach. Given the short timeframe for achieving compliance, you should focus initially on the most significant gaps, given the specificities of your organisation, and try to leverage as much as possible the ongoing measures defined to close the gaps to the GDPR's requirements.



Holistic approach

Leveraging as much as possible the existing activities under GDPR framework will help banks ensure consistency in their regulatory response and help increase the efficiency of their change management

How can PwC help?

- We can help clarify what the ePR is, which requirements are relevant to the banking industry and how they affect your organisation – both before and after the date of adoption.
- We have expertise in conducting readiness tests in relation to GDPR and we can assist you in identifying weaknesses and gaps relating to ePR requirements.
- We can provide the tools and assessment frameworks to help you understand how compliant you are with the ePR requirements.
- We can provide you with access to a global, multidisciplinary team that has extensive cross-sector expertise in risk assurance, programme assurance as well as legal, forensics and data protection.
- We can support you with the development of a strategy for investment in privacy protection and give you recommendations on how to approach the management of activities relating to ePR compliance, including governance and reporting aspects.
- We know which requirements, challenges and threats are relevant for the banking industry and can assist you in identifying the aspects that matter most to your organisation.
- Our team can support you with your preparations for ePR compliance by ensuring that your employees and your suppliers are trained and aware of their responsibilities in regard to the new regulation.
- We have extensive experience implementing GDPR privacy strategies in the banking sector and can leverage this knowledge to help you ensure timely compliance with the new ePR requirements.

For more information, please contact:

Regulatory Transformation

Patrick Akiki
Partner,
Finance Risk and Regulatory Transformation

+41 79 708 11 07
akiki.patrick@ch.pwc.com

Morris Naqib
Senior Manager,
Finance Risk and Regulatory Transformation

+41 79 902 31 45
morris.naqib@ch.pwc.com

Legal

Günther Dobrauz
Partner,
Legal FS Regulatory & Compliance Services

+41 79 894 58 73
guenther.dobrauz@ch.pwc.com

Philipp Rosenauer
Manager,
Legal FS Regulatory & Compliance Services

+41 79 238 60 20
philipp.rosenauer@ch.pwc.com

PwC Digital Services (PDS)

Reto Haeni
Partner,
Cybersecurity and Privacy

+41 79 345 01 24
reto.haeni@ch.pwc.com

Nicolas Vernaz
Director,
Data Protection and Regulatory Compliance

+41 79 419 43 30
nicolas.vernaz@ch.pwc.com

Key contributors:
We would like to thank Isabella Sorace and Mateja Andric for their valuable contribution to this publication

Notes