www.pwc.ch/

Is the insurance industry ready for the ePrivacy Regulation?

The disruptive impact of the ePrivacy Regulation (ePR) on insurance companies

"We care about the user experience. And we're not going to traffic in your personal life."

Tim Cook

pwc

Table of Contents

The ePrivacy Regulation (ePR) and its impact on insurance companies

The European Commission is finalising the ePrivacy Regulation (ePR)[1], which may become effective by the end of 2018. The ePrivacy Regulation, 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. Although many insurance companies are already changing their digital strategies, the ePR will have a disruptive effect on the industry.

ePrivacy Regulation in a nutshell

The ePR will replace the existing ePrivacy Directive[2], which was revised in 2009. The new regulation includes several modifications to address current trends in digital markets and it entails a considerable extension of scope. The key goal of the ePR is to protect electronic communications of natural and legal persons and to protect the information stored in those persons' terminal equipment.

Legal background

In 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. Such services 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, for example, text messages, emails 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 contents and metadata is conditional on consent**
  Privacy is guaranteed for the contents of communications as well as metadata; for example, who was called, the timing, location and duration of the call, as well as websites visited.

- **Spam and direct marketing communications require prior consent**
  Regardless of the technology used (e.g. automated calling machines, SMS or email), 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.

1 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

2 Directive 2002/58/EC and the 2009 update, Directive 2009/136

Key requirements of the ePrivacy Regulation

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

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

- **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 data must be deleted once they are no longer needed for the 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 ePR 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 related 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 enable 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 email, calls or any other electronic service).

- **Transparency on security risk**
  Providers of electronic communication services have to inform users about 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 in 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 note 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 that they do not lower the level of protection enjoyed by natural persons under the GDPR).

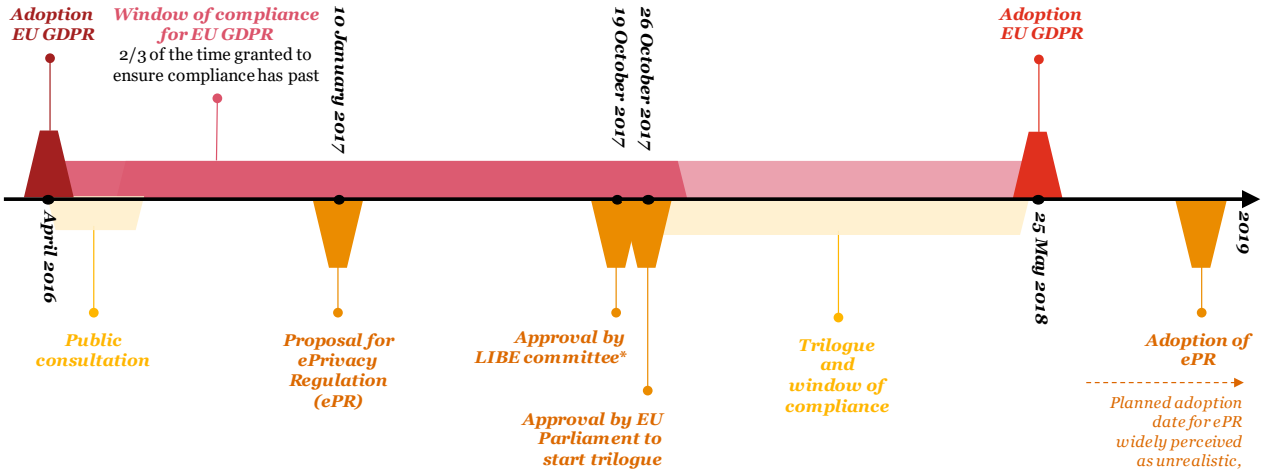
In light of the above, the following considerations are vital to the efficient and successful analysis and implementation of the two regulations.

Shared backbone

Due to their complementary nature, the two regulations share a number of similarities, most notably their national transposition model: both the GDPR and the ePR 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.

One difference between the two will be the date of application as the consultations of the 'trilogue' (i.e. the European Parliament, the European Council and the European Commission) have not yet finished. Therefore, the ePR will not be applicable from 25 May 2018, as is the case for the GDPR. It is still not clear when the ePR will be adopted, but it is expected to be by the end of 2018 according to the European Parliament.



** 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 EU, 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 EU • Personal data of subjects in the EU	Electronic services provided to users in the EU (location where the user uses the service)	Widening of territorial scope to use of electronic communication services in the EU

Complement to the GDPR

In addition to extending the scope of applicability to legal persons, the ePR introduces additional requirements that ensure an increased level of protection on the data of natural persons, as outlined 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 grounds	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 now, 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 EU (including Switzerland)	Applicable to non-EEA entities if they provide goods or services to data subjects domiciled in the EU.	Applicable virtually to any entity with a website or an app, unless access to them is restricted for users within the EU (i.e. if your clients can access your website from an EEA country, then your entity must comply with the ePR)

How does the ePrivacy Regulation affect you?

Insurance companies manage, as part of their core business, a significant amount of personal data – often data that are classified as sensitive under the GDPR (and thus subject to stricter requirements). As such, the industry has been strongly affected by the upcoming GDPR and compliance measures have been defined and implemented in most companies. These will be the starting point for meeting the ePR's requirements; however, more effort will be needed, especially considering the recent technology-driven developments in the insurance market.

Key challenges of ePR for insurance companies

At the core of their business, especially in the Life segment, insurance companies collect and process large volumes of personal data. Consequently, technological developments in the area of data management have become a key to success in the industry – even more so, given the impending arrival of the GDPR. As the ePR also protects legal persons, insurance companies will be just as heavily impacted as other segments with regard to the management of confidential data as a whole.

The insurance market relies heavily on the electronic processing and transmission of personal and confidential data, with an increasingly large footprint in the IoT environment. As such, there is a risk of disruption due to the adoption of the ePR. One way to survive such disruption is to prepare for it. To this end, we've made a list of the key challenges arising from the requirements set down in the draft ePR.

- **Protection of legal persons**
  In the exercise of their day-to-day business, insurance companies 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 containing personal or confidential data, and this will translate into additional measures to ensure the protection of such data.

- **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. Insurance companies are showing increasing interest in the IoT in an attempt to become more competitive in the market. The ability to track the behaviour of clients could enable insurance companies to offer better prices to 'more conscientious' individuals. The ePR will protect the data collected and stored using these new technologies, so insurance companies will have to comply with the stricter requirements.

- **Protection of electronic communication**
  The ePR aims to protect all kinds of data processing within the scope of electronic communications. Like any other modern industry, insurance relies heavily on electronic communication. However, good management and control of these communications is vital in the insurance market: companies are finding new ways to certify their communications, especially those relating to claims. Some innovators are also trying to redefine the entire claims process, for example, with the use of a blockchain. Although this may make the entire process more efficient and less subject to fraud, adequate preparation is needed to ensure that the electronic communications involved in such a process comply with the ePR.

- **Metadata restrictions**
  Certain companies are considering how to use metadata to improve their underwriting process. Using data such as geo-location information (obtained, for example, from monitoring the use of websites or applications) could help in identifying smaller and smaller homogeneous pools of risk, which would increase the reliance of risk models. However, the ePR will introduce restrictions on the processing and/or storage of metadata, which may negatively affect the sort of innovations insurance companies are currently looking into.

- **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 emails and voice calls, but also all the 'Over-the-Top' (OTTs) 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. As described above, insurance companies are investing in the IoT, blockchain and other innovative technology. For any such new technology, insurance companies should consider the additional R&D budget needed to comply with the ePR's requirements (cost of compliance).

- **New regulations on cookies**
  Insurance companies may use cookies to offer to individuals products targeted to their specific behaviours (for example, a user who often visits travel websites could be offered travel insurance by the insurer). 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 insurance companies and the effectiveness of their targeted online advertisements.

- **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 will require prior consent by the employees and, potentially, by any user communicating with the insurance company. This would require insurance companies to review thoroughly their current screening practices.

What is our suggested approach?

Although the final text of the ePR is yet to be published, insurance companies could start assessing their readiness in relation to the draft regulation, as this would position them well when the definitive text is published.

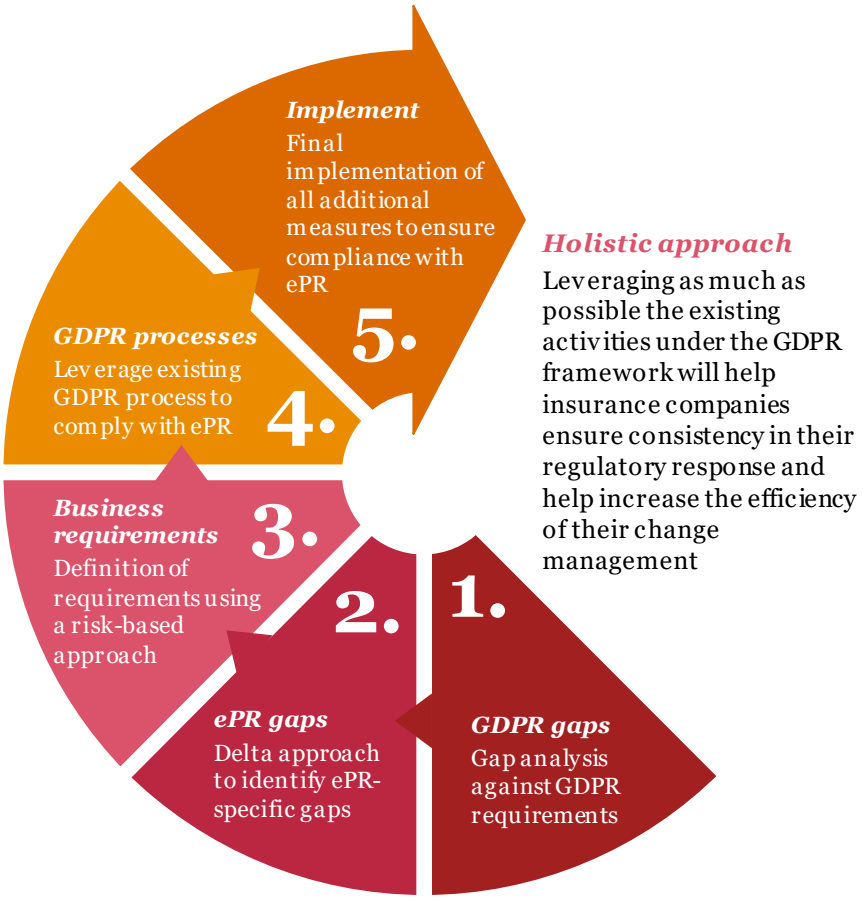
Prioritisation is key

In order to ensure an adequate prioritisation exercise, it is important first to understand how the ePR affects your company. 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 company 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 company 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 insurance 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 the GDPR framework will help insurance companies 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 insurance 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 the 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 insurance 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 insurance sector and can leverage this knowledge to help you ensure timely compliance with the new ePR requirements.

For more information, please contact:

Patrick Mäder
Partner,
FS Europe Leader

+41 79 18 01 04
maeder.patrick@ch.pwc.com

Patrick Akiki
Partner,
Finance Risk and Regulatory Transformation

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

Morris Naqib
Senior Manager,
Risk and Regulatory Transformation

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

Key contributors:
We would like to thank Isabella Sorace and Pedram Rostami for their valuable contribution to this publication.