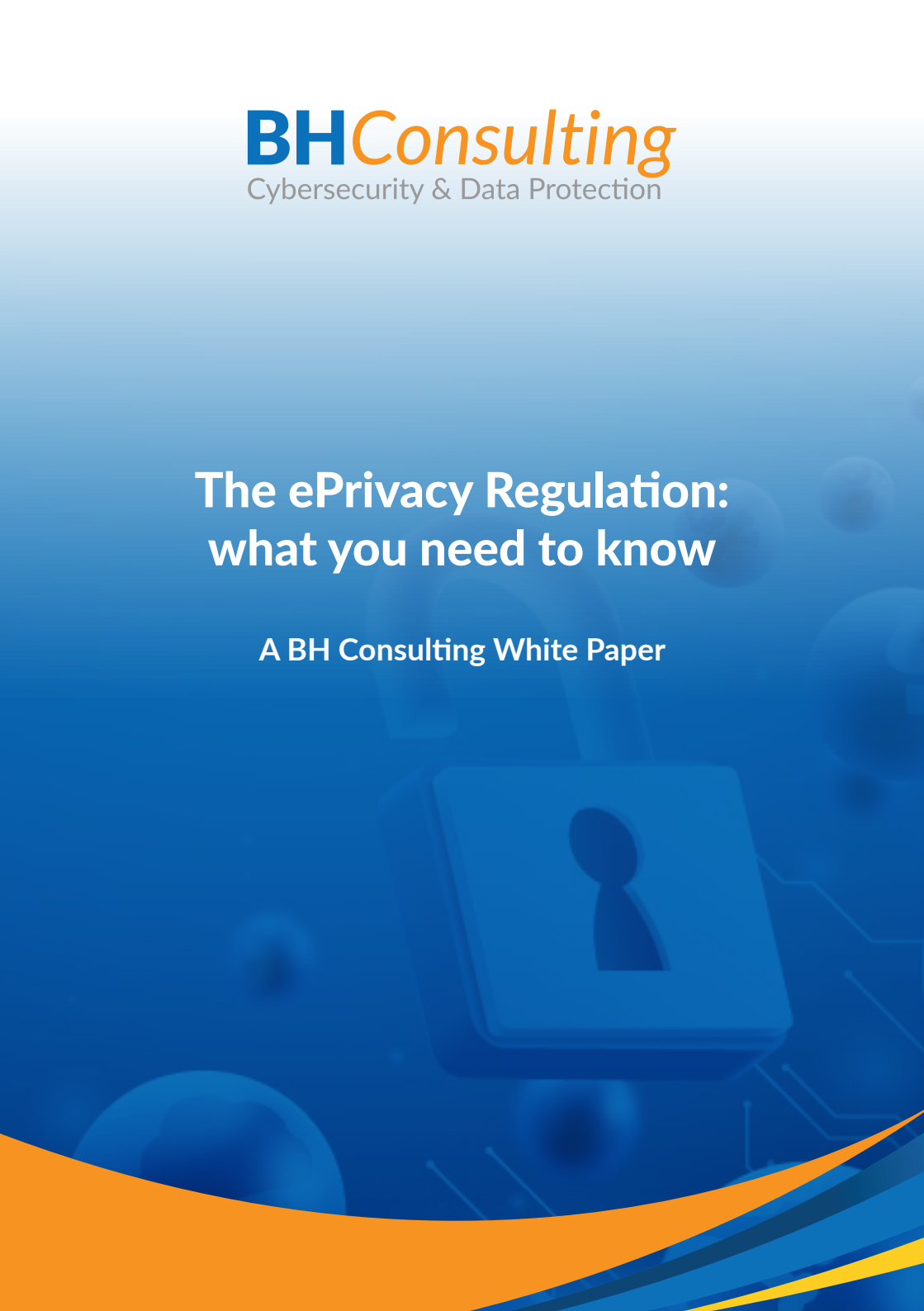
BH Consulting
Cybersecurity & Data Protection

The ePrivacy Regulation: what you need to know

A BH Consulting White Paper



About this guide

Businesses and public organisations have many ways to communicate with and market to their customers. In today's post-pandemic world, digital channels such as websites have taken on even greater importance at a time when people had to restrict their movements.

At the same time, instant and social media messaging services and 'voice over internet protocol' VoIP providers have grown in popularity in recent years; WhatsApp alone has 2 billion users. Many companies have been quick to seize the cost-effective ways to increase their brand's reach through digital channels and, in theory, create closer relationships with current or potential customers – but they must do so lawfully.

Against this backdrop, the ePrivacy Regulation (ePR) is coming, and it will have a huge say in how companies communicate and market to customers, and how they track activity on their websites through cookies.

Once it comes into force, the new regulation aims to ensure privacy in all electronic communications. It is an update that takes account of the many changes in technology since its predecessor, the ePrivacy Directive, was passed in 2002.

However, the regulation has been delayed due to discussions on a number of contentious issues. The most recent update on February 10, 2021 was to positive step forward where European Union member states agreed on a negotiating mandate for revised rules to finalise the ePR which allows the current Portuguese presidency to start talks with the European Parliament on the final text.

Recent debate over the changes, together with a likely 24-month implementation period, mean that the updated version is unlikely to take effect until 2023. Fortunately, this timeframe gives organisations sufficient notice to become familiar with what the regulation will require, understand how it will affect their communications, and start preparing for its arrival.

At BH Consulting, we believe complying with privacy regulations should not just be a tick in the box exercise. Having a proactive and positive approach to digital privacy can increase trust from customers and potentially be a competitive differentiator. That is all the more reason to start preparing for ePR now.

This white paper will describe some of the context for the regulation, how it complements (or supersedes) the EU GDPR, and summarises the latest developments. We are aiming to make the paper as relevant as possible, while acknowledging that the regulation is still in draft form. If there are substantial changes to the text before it is approved, we will update this white paper in due course.

What is the ePrivacy Regulation?

The purpose of the ePrivacy Regulation (ePR) is to modernise the ePrivacy Directive 2002/58/EC (amended 2009/2011) by updating the rules to reflect significant technological developments and ensure it complements the EU General Data Protection Regulation (GDPR). The EU's EUR-Lex website tracks the progress of the regulation and publishes all drafts for anyone to read.

The European Commission first proposed the regulation in 2017 to "reinforce trust and security in the digital single market". The broad aim of ePR is to enhance communications security, confidentiality and privacy, to define clearer rules on tracking technologies, and to try and harmonise the approach across all EU Member States, as the GDPR has done.

Where the GDPR relates to the processing of personal data that could identify an individual resident in the EU, the ePR goes further in certain cases, such as creating specific new rules on the right of confidentiality and data privacy and protection in areas of electronic communications like business-to-business direct marketing. The ePR is intended to take precedence over GDPR in cases where both laws apply.

In a similar way to the GDPR, the ePrivacy Regulation has an extra-territorial application, which means it can apply regardless of whether the provider of an electronic communications service is established in the EU.

The term 'electronic communications' is worth further comment, as it is purposely broad and intended to cover:

- Websites (e.g. cookie notices)
- Email (e.g. direct marketing, spam etc)
- Online Advertising
- Apps
- Telecoms
- Instant messaging
- The Internet of Things (e.g. gathering data through embedded sensors)

Why is it being updated?

In simple terms, a lot has changed since 2002. Back then, there was no Facebook, no iPhone or WhatsApp, and email was not the pervasive marketing tool it is today. The regulation is being broadened out to bring it up to date with new technologies and digital channels that have emerged and become popular in the interim, such as instant and social media messaging services like WhatsApp and Snapchat, and voice over internet protocol (VoIP) providers such as Skype, and also to regulate electronic marketing communications.

In addition, EU Member States can incorporate a directive into their own national law and interpret it individually. A regulation, unlike a directive, automatically comes into effect as legally binding in all Member States.

The EU's approach in defending the individual's right to privacy has led to restrictions on how online service providers and social networks, such as Google and Facebook, track people on the internet. But although the General Data Protection Regulation has been in force since 2018, there have been delays to the arrival of the ePrivacy Regulation.

Why is the regulation not in force yet?

The proposed 2017 revision drew criticism from several EU Member States. Two years later, in July 2019, the Finnish Government issued a revised proposal with some amendments relating to the content of electronic communications, data and metadata – which is likely to include location data – as well as further processing of metadata.

However, this draft proposal was defeated in late November 2019 in a vote by Member States. Opinions differed on key areas ranging from cookie tracking, consent, and compliance with the GDPR, to the processing of electronic communications data by third parties. European Digital Rights expressed concern over the rejection, with its head of policy Diego Naranjo stating his concern that the revision is "protecting online tracking advertising and big tech".

On 20 November 2020, the Presidency of the Council of the European Union released its progress report on the Proposal for a Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (the Draft ePrivacy Regulation).

In particular, the report recalls that the German Presidency proposed, among other things, to remove, as a legal basis, the legitimate interests of an electronic communications network or service provider as a legal basis for processing of electronic communications metadata or for using processing and storage capabilities of terminal equipment or collecting information from an end-users' terminal equipment. In addition, the report highlights that the Presidency proposed to delete specific data retention issues in view of the Court of Justice of the European Union's ('CJEU') judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.

However, the report notes that while Member States broadly supported the deletion of 'legitimate interests' as legal basis, they also noted that the text was too restrictive towards innovation and the permission for processing of metadata, among other things. Furthermore, the report provides that a number of Member States expressed the view that the Finnish Presidency's proposal could be considered as the starting point for future negotiations, that it is clear from the Member States' reactions that further work is needed on the file, and that the German Presidency is committed to working closely with the forthcoming Portuguese Presidency to facilitate further discussions and to ensure smooth progress on the file.

One of the objections appears to hinge on claims that the ePR, as currently conceived, would hinder investigations into online child abuse. The European Commission had proposed a temporary derogation from the ePrivacy Directive for the purposes of combatting child sexual abuse online. However on 11 November 2020, the European Data Protection Supervisor, the EU's independent data protection authority, published its Opinion on the move, stating:

"...the measures envisaged by the Proposal would constitute an interference with the fundamental rights to respect for private life and data protection of all users of very popular electronic communications services, such as instant messaging platforms and applications. Confidentiality of communications is a cornerstone of the fundamental rights to respect for private and family life. Even voluntary measures by private companies constitute an interference with these rights when the measures involve the monitoring and analysis of the content of communications and processing of personal data. The EDPS wishes to underline that the issues at stake are not specific to the fight against child abuse but to any initiative aiming at collaboration of the private sector for law enforcement purposes. If adopted, the Proposal, will inevitably serve as a precedent for future legislation in this field. The EDPS therefore considers it essential that the Proposal is not adopted, even in the form a temporary derogation, until all the necessary safeguards set out in this Opinion are integrated."

The full text of that opinion is available here.

https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-proposal-temporary-derogations-directive_en

Further complications arose following the outbreak of COVID-19, because some Member States' governments envisaged using mobile location data as a possible way to monitor, contain or mitigate the spread of the virus. This would imply the possibility of geolocating individuals or to send public health messages to individuals in a particular area by phone or text message.

What will it cover?

The agreement by the EU Member States on February 10 now outlines the main areas to be addressed by the ePR:

1. Inclusion of location metadata. 'The regulation' now includes the possibility of including the processing of metadata and to regulate the processing of metadata which is location data. This may include the processing of metadata for billing purposes, to protect vital interests or in preventing or detecting fraud. This will provide for the conditions and purposes for processing.
2. Provision is included for machine-to-machine data transmitted via a public network (to promote a safe Internet of Things)
3. The confidentiality of electronic communications is reinforced
4. Conditions where the permitted processing of communications without user consent may occur will be included
5. The ability to use data from a user's terminal equipment will require consent or under specific purposes
6. The need for genuine choice for cookie consent will be reinforced
7. The potential to manage "cookie fatigue" for users where user may be able to consent to certain types of cookies by whitelisting certain types in their browsers

The document also includes requirements about online identification, public directories, and unsolicited and direct marketing.

How will the ePR be enforced?

The ePrivacy Regulation is adopting the same structure of financial penalties as the GDPR. Organisations found in breach of ePR may be fined up to €20 million, or 4% of their global turnover, whichever amount is higher. As with the GDPR, individuals affected by a breach of the regulation will be entitled to recover damages.

Under the ePrivacy Directive, a breach is a criminal offence and may lead to a court-imposed fine. Under the new regulation, the fine will be higher and the supervisory authority (such as the Data Protection Commission (DPC) in Ireland or the Information Commissioner's Office (ICO) in the UK) can impose fines directly without needing to go through the courts system.

What's next?

The Council will now begin discussions with the European Parliament to negotiate the final text. There will be a 24-month implementation period once the ePR has been approved which means that the updated version of ePR is unlikely to take effect until 2023.

What will it look like in practice?

As stated above, the wording of the new regulation has now entered the final stages of being approved as this white paper is being written (February 2021) and is still subject to change. Nevertheless, based on material already in the public domain, it's possible to make some general observations on what the regulation will require companies to do.

The 2002 ePrivacy Directive and its 2009 update came to be known as the 'cookie law' because of how it led to cookie consent notices popping up on websites more frequently – often to the user's annoyance.

The Commission proposes that where cookies process information anonymously, they no longer need end-user consent. So in theory, that should lead to fewer pop-up messages or cookie walls for end users, and a better digital experience – all while continuing to uphold individual privacy and protecting the confidentiality of their computing or browsing devices.

According to research published in 2019, more than 60 per cent of popular websites in Europe display cookie consent notices to visitors since GDPR.

There are three main types of cookie notices: one gives the website visitor a simple yes or no choice, as to whether they agree to cookies on their laptop or mobile device. This doesn't penalise the visitor who clicks 'no'. They freely choose to give their consent or not and are free to browse that website regardless of their choice.

The second type of cookie partially penalises the user, in that some website functionality won't work if they choose 'no'. However, a properly worded cookie notice should make clear to them exactly what functionality won't work. Here again, the individual can make an informed choice to proceed or not.

In the third case, a 'cookie wall' is established, denying the user access unless they consent to all cookies and trackers that are present on that website. A cookie wall is a website's self-made border that restricts access to those who do not consent to all of its cookies and/or tracking technology. The controller is essentially forcing the data subject to provide access to their personal information.

However, a cookie wall is an ambivalent construct, with some data protection authorities in the EU already deeming them unlawful. The Dutch regulator's website highlights that cookie walls are not permitted, because with a cookie wall the controller cannot get valid permission from visitors/users for placing tracking cookies.

What do I need to do?

The rules regulating cookies are still being set, and cookies themselves are continually evolving, which means maintaining a current cookie policy will be a continuous job. However, properly informing your users about the cookies your site is using and, when necessary, receiving their consent will keep your users happy and keep you GDPR-compliant.

As with many things, there's the letter of the law and its spirit, and they might not always be the same. Do cookie consent notices tell individuals everything that's happening with their data? A major study of cookie consent mechanisms by academics at Ruhr-University Bochum and the University of Michigan found that 86 per cent of notices offer no options other than a confirmation button that does nothing.

So, what should organisations do to make their actions more transparent?

In essence, cookies cannot truly use 'consent' as their legal basis for processing, as they penalise the user who says no, by preventing the user from accessing the

website. The GDPR defines valid consent as being freely given and warns that consent will be invalid if it is conditioned upon the exchange of a service to which the data processing is not necessary.

The practice of cookie walls, along with the general confusion among consumers, hasn't escaped the notice of supervisory authorities. Both the Irish DPC and UK ICO have issued guidance on correct use of cookies. Johnny Ryan from the privacy browser Brave issued a formal complaint to the Irish DPC in April 2019 against Interactive Advertising Bureau (IAB) Europe's website cookie wall – which forced visitors to accept tracking cookies.

Not all cookies require consent: the ePrivacy Regulation allows for exemptions where cookies are used only for carrying out the transmission of a communication or where they are strictly necessary to provide a service. The recent guidance from the DPC makes this point clear. It says: "For the setting use of cookies and other similar technologies, the data controller normally needs your consent (as required by regulation 5(3) of the ePrivacy Regulation) to use these types of technologies. However, they don't need consent where the cookie or other technology is necessary to provide you with the service you're seeking [our emphasis] – for example, cookies which may be needed to provide you with a functioning website which you want to access." (The European Commission page on cookies also has more information about this).

Best practice cookie notices

What should organisations do to ensure they are complying with both the letter and the spirit of the laws regulating the use of cookies? The first step is to determine if the principles of GDPR and ePrivacy Regulation are applicable, by assessing if your website cookies:

1) collect or process personal data from individuals resident in the EU, or

2) collect or process data on servers located within the EU?

If so, it is worth asking these questions:

- Are you being transparent with the data subjects?
- Are data subjects fully informed about the collection and processing of their data and the possible sharing of their data with third parties and for what purposes the sharing will take place?
- Would data subjects be 'surprised' by any activity your cookies undertake? If so, you should revisit the privacy notices and ensure increased transparency.
- What legal basis are you using to collect and process this data? Are you using consent as the legal basis? If so, does the data subject have a choice? Does the data subject feel coerced in any way? Does the data subject provide a positive affirmative opt-in?
- Is the 'informed' piece being delivered in a 'terms and conditions' link, a 'privacy policy' link– or really clearly on a privacy notice appearing on-screen beside the cookie consent request?
- Is the information you intend to gather proportionate and necessary for the visit the data subject is making to your website?

- Do you need this information for your website to function properly?
- Is this the right time during the transaction/visit to collect or process the information? Do you need to wait until a contract (implicit, social or otherwise) is engaged in by the data subject?
- Are you collecting/processing data subject's information to leverage it for future use?
- Are your retention schedules clearly outlined and are you deleting information in line with them?
- Do the privacy notices make it easy for the data subject to get more information/communicate with your privacy department if they wish to ask for more information?

Many privacy notices appear boilerplate and lack transparency. It is not hard to imagine that this gives consumers a lack of confidence that data controllers are complying when they click 'no', or 'reject all', after a cookie notice.

A notable trend in this area is the 'Consent-or-Pay-Wall'. Pay models are an alternative to the ad-funded/information collection model. They allow a non-consent (contractual agreement) based alternative if the consumer pays.

Why not provide clearly worded notices that state in simple language what is happening to a visitor's data? Why not use cookie consent as a method to enter into an implicit understanding that engenders trust? For example, "in return for giving us your information, you will get a better experience on this website.

We promise to only use that information during the time you're using it, and we will delete it afterwards. We will never share information from your visit to our website with third parties".

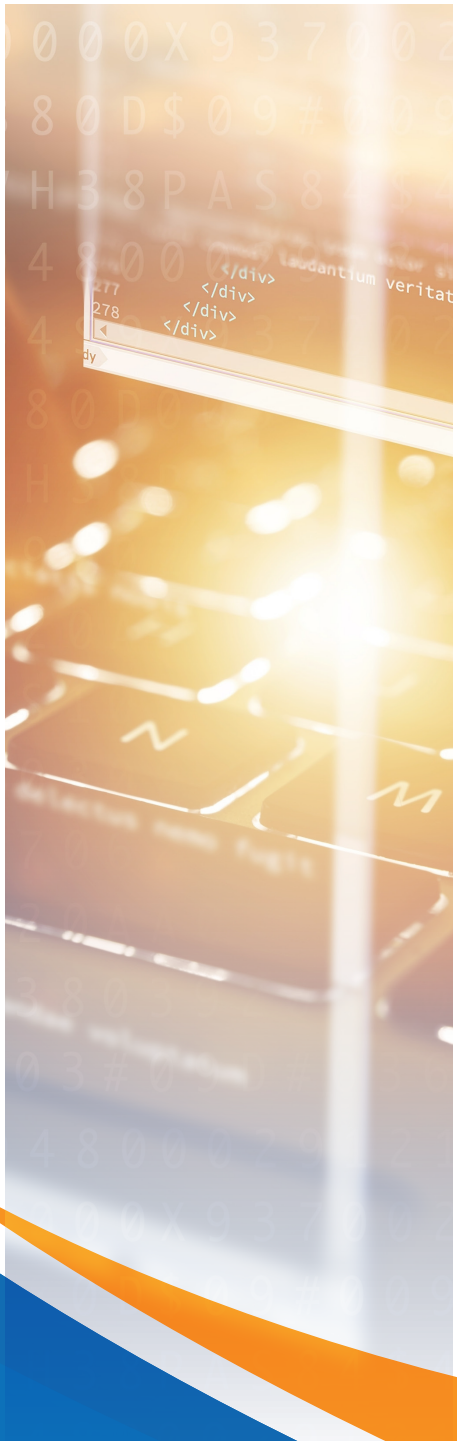
Whatever way an organisation chooses to design and use its cookies, it is worth remembering that a website shines a light on that organisation's data protection practices. Companies should consider their privacy notices and the level of consumer loyalty and engagement that these notices engender, as studies have found correlations between well-constructed privacy notices and increased consumer trust.

What ePR means for marketing communications

Article 16 of the Commission's draft states that end users may not be sent direct marketing communications unless they have given their consent.

There are several exemptions to this, including marketing to existing customers, and sets out rules for marketers, including the obligation to reveal their identity and provide the opportunity for recipients to opt out of further marketing communications.

The Council's latest draft amends Article 16 to refer to 'unsolicited' as well as direct marketing communications. It also adds the option for member states to set a time limit after which organisations may not send marketing communications to their customers.



Note that, although the GDPR states in Recital 47 that "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest", the ePrivacy Regulation, as 'lex specialis' to the GDPR's 'lex generalis', will overrule the GDPR, so if the final version requires consent, legitimate interests will not be valid for direct marketing even though the GDPR says they are.

What do I need to do?

End users will also have the absolute right to object, in which case you must stop marketing to them as soon as possible, but certainly within one month. You must also inform them of that right, as well as the fact that you intend to use their data for direct marketing purposes.

What is not covered?

The ePrivacy Regulation will not apply to, among others, electronic communications data that is processed after receipt by the end-user concerned and data processing activities related to the prevention, investigation, detection, and prosecution of criminal offences.

Conclusion

The stated reason for the existence of the ePrivacy Directive is to "reinforce trust and security in the digital single market". Arguably the first element of that aim is incumbent on companies to which the regulation applies, because their approach will ultimately determine whether the ePR achieves its aim or not. With that in mind, we believe they should do more than just the bare minimum needed to comply with ePR. Companies can – and should – go further by being clear and transparent with their users or customers about how they intend to use their data.

Just as the GDPR gave notice well in advance of any notice period, the ePrivacy Directive looks set to do the same. So now is the time to prepare. Data protection and privacy, when done right, gives companies a unique opportunity to engage with consumers and demonstrate that company's socially responsible data strategies. By ensuring that those strategies, including those relating to cookies, are benevolent towards the data subject, organisations have a valuable opportunity to do privacy right, and enhance the trust relationship with consumers.

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie