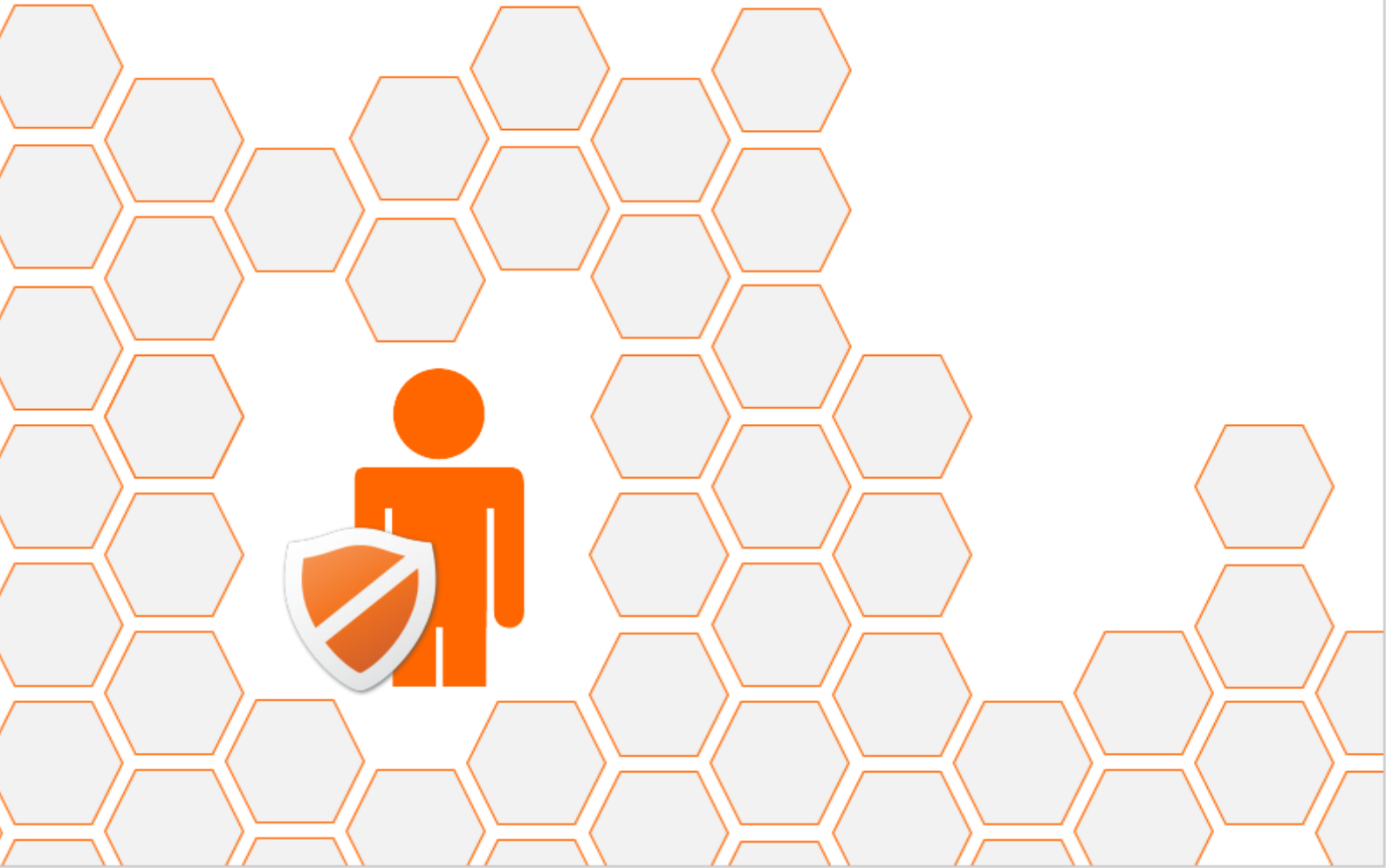
Intermedia Global

GDPR 2018

The information you need to know



Contents

GDPR in the Workplace

The GDPR deadline of 25th May 2018 seems like a distant waypoint, but it's not when you consider what many businesses are now having to go through: a fundamental restructuring of the way they collect, process and use any personal data in their business.

The General Data Protection Regulation, GDPR, is a result of a decade of negotiations aimed at further protecting the privacy rights and interests of citizens. It replaces all data protection laws for EU members, including the UK's own Data Protection Act (1998). Due to the timescale of Brexit and the GDPR, it new data protection regulations ***will*** apply before the UK has left the EU.

Accountability and Responsibility

Those two words should echo around an organisation's board room from now on with this new regulation. An organisation should be asking itself questions such as: What types of personal data do we hold? Where is it located? How accessible is it? Are we adequately protecting the data? Are we adequately protecting the target's rights and interests? Do we have the necessary consent? Most importantly: **Are we compliant?**

Data protection should become a board-level discussion due to the huge onus on organisations to comply, and the penalties for those who don't. Where the DPA (1998) was typically tougher on companies operating inside the EU, the scope of **GDPR extends globally**. If an organisation holds or processes data that can identify an EU citizen, then they must comply regardless of physical location.

It also brings data processors into the spotlight. While the GDPR still focuses on the controllers i.e. who collected it and who dictates its use, data processer such as data suppliers are also brought under the microscope when it comes to accountability.

Key Areas

Consent

During the DPA era, many businesses relied on 'implied' consent. This passive approach was taken advantage of over the following decade until it was rewritten during the negotiations for the GDPR. A pre-ticked box stating they subscribe, or allow 3rd parties to use their data was often used – and if the consumer didn't bother to untick the box, then implied consent was given.

The GDPR however states that a "clear affirmative action" needs to happen for consent to be valid. This will mean actively ticking an un-ticked box for consent. This however, for clarity and safety's sake should be followed up by an email – "click here to confirm subscription" for example. This created the double opt in and is a clear sign they want their data used by the company.

Right to be Forgotten

Consumers have the right to request their data be deleted thanks to the GDPR. Any personal data stored on the subject must be deleted unless there is a legitimate need for the business to keep it.

Data Protection Officers (DPO's)

While the requirement to appoint a DPO is new under the GDPR, it has been a long-standing element of data protection in Germany. Modelled on that, a modified version made its way into the GDPR.

Companies are required to appoint a DPO if they process vast quantities of personal data on a regular basis or they process on a large scale 'special categories' data (e.g. race, religion, health – anything deemed sensitive)

Breaches & Penalties.

The punishment for data breaches has been dramatically increased from the £500,000 maximum fine that was permitted under the DPA. The GDPR provides a comprehensive package for collecting, processing and managing data and should therefore not be violated. Heavy fines of up to 2% of annual global turnover await those who fail to comply with GDPR. Businesses who suffer a serious data breach are open to fines of up to €20m or 4% of annual turnover – whichever is higher.

What constitutes a breach?

Words like hacking, cybercrime and data breach often send alarm bells ringing amongst business leaders around the world. That's because it's become a very serious issue in the digital age, with data breaches posing a real threat to the subject's privacy and rights.

A data breach is more than just losing personal data. A Breach, as defined by the ICO is:

"A breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

Breaches vary in severity which makes it important to understand how an organisation has been breached, what has been accessed and how it will affect the rights of the subject(s). Not all breaches need to be reported, in some cases it can be handled internally without notifying supervisory bodies. However, when the breach will likely have a "significant and detrimental effect on individuals" then it **must** be reported.

For example, a data breach which allows unauthorised access to customer's transactional data risks the subjects falling victim to identity theft. This should be reported as it imposes a threat on the security of an individual. Accidently altering staff telephone numbers on the other hand can be handled in house and not worth reporting.

[B]2B, or not to 2B?

There has been longstanding confusion over the rules and how they apply to the marketplace. Let's first look at the two landscapes and then divulge into what's changed and how so.

Originally the distinction between B2B and B2C were based on the context in which the subject was categorised. Targeting a 'natural person' meant targeting a normal human being, whereas targeting a 'legal person' meant a business or legal entity. The B2B sector was typically less regulated because it encouraged business relationships, sales and therefore economic growth.

Expanded definition of personal data

Personal data now has an expanded definition, going as far as to say that even IP addresses count as personal. Anything that can identify a citizen of the EU is considered personal data. Standardised addressed such as sales@, info@ or enquiries@ are not considered personal data, but if an email address contains information about an individual e.g. [first name].[last name]@Intermedia-global.com then it will be personal data.

Although that seems straight forward, we now must consider the context in which those emails are being used.

Sole Traders & Partnerships Vs Plc, Ltd & Local Authorities

Hypothetically speaking, if one knows for a fact that Intermedia Global is a sole trader or partnership then they must seek opted-in consent to target via emails or sms, unless they have previously purchased from the company. Sole traders & partnerships are covered under the same core opt-in principles as B2C.

On the other side, if one knows that Intermedia Global is Public/Private limited company or a local authority there is precedent to communicate on an opt out basis. However, one should tread carefully in this area because there are two interpretations of the GDPR regarding opt-in/opt-outs.

Consent Vs Legitimate Interest

Despite knowing the extent to which the term ‘personal data’ applies and the differences between the various business categories stated above, it’s more important to understand consent vs legitimate interest perspective.

Consent

If a business decides to go down the consent route, then it would need to gather opt-in permission from all contacts. This is the safer option of the two as it guarantees compliance. This isn’t to say the legitimate interest route means non-compliance. On legal grounds, it may be a safer option to ensure all contacts are opt-in rather than rely on an interpretation of legitimate interest.

Legitimate Interest

“If a business decides to use the legitimate interest precedent for their direct marketing, then it will be able to send email marketing on an unsubscribe/opt-out basis” - DMA

This may seem like a “get out of GDPR free card” but it is not. Firstly, the organisation still must comply with every other aspect of the GDPR. Secondly, legitimate interest is open to interpretation, which is good from a marketer’s perspective but troublesome from a legal perspective.

Choosing the consent route, providing the organisation has records of opt-in time/date, is a legally protected route. If challenged, it may be significantly hard to prove legitimate interest.

Opt-in/Opt-out by Channel

Legitimate Interest

Channel	B2B	B2C *(Inc Sole Traders & Partnerships)*	Notes
Mail	Opt-Out	Opt-Out	Check against MPS
Telephone	Opt-Out	Opt-Out	Check against TPS & CTPS
Email	Opt-Out	Opt-in	
SMS	Opt-In*	Opt-in	*No way of differentiating between B2B/B2C so treat as if B2C

This is similar to what marketing practices currently operate under. The main difference here is the fact that sole traders and partnerships will be opt-in come 25th May 2018.

Consent

Channel	B2B	B2C *(Inc Sole Traders & Partnerships)*	Notes
Mail	Opt-in	Opt-in	Check against MPS
Telephone	Opt-in	Opt-in	Check against TPS & CTPS
Email	Opt-in	Opt-in	
SMS	Opt-in*	Opt-in	*No way of differentiating between B2B/B2C so treat as if B2C

Although telephone and mail channels may be opt-out, if your business adopts a 'consent only' approach this would require consent across all channels regardless of B2B or B2C sectors. The benefit of which completely covers a business from any opt-in/out disputes by only targeting those who are opt-in. On the other hand, it could prove difficult to expand one's customer base.

Sources:

https://dma.org.uk/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

Intermedia Global will continue to update you on the latest developments from the EU regarding data protection and the GDPR, in the run up to May 2018

Our team of data protection experts are on hand to support any requirements or questions you may have regarding data protection and GDPR.

Please do not hesitate to contact us for further advice and information.

Tel: +44 (0)1234 831000

Email: Info@Intermedia-global.com

Intermedia Global Ltd
17 Stephenson Court,
Fraser Road
Priory Business Park
Bedford
MK44 3WJ