Omega
Global Resource Solutions

GDPR: 10 REAL LIFE SCENARIOS

AN EXPLORATION OF BUSINESS-CRITICAL SCENARIOS AND ACTIONS

Guide Overview:

In our last guide, we explained the fundamentals of the GDPR and how best to prepare for the forthcoming changes, including a 10-point action list to consider.

As the due date draws nearer, there are still a number of unanswered questions and confusion around some areas of the GDPR. We have created a guide that pursues those areas, giving a detailed explanation to each question and a recommended action point.

Included in this guide:

- 10 key questions and answers
- A key employer action for each question
- Information on the ePrivacy directive

1 Can I still use opt-in consent forms on my website?

Under the GDPR, a person gives consent "by a statement or by a clear affirmative action", which might include: ticking a box when visiting a website (pre-ticked boxes do NOT constitute a clear affirmative action), choosing technical settings for information society services or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the processing of their personal data.

Whilst there is not yet a recommended confirmed approach to ensure a consumers' "clear affirmative action" for GDPR compliance, the best current option is the double opt-in process.

The double-opt in process includes:

- Inbound marketing technology that enables sign-up forms to be embedded on a website
- Follow-up email automation that includes a confirmation link that will complete the double opt-in
- Audit-trail capability to ensure that each opt-in action is recorded and stored as evidence of their consent

Investing in an efficient CRM system that includes form creation, email automation and an audit-trail function is the best solution to ensure transparency of customer consent

KEY EMPLOYER ACTION

Ensure that you have double-opt in functionality on all web forms prior to the GDPR implementation date.

2

What is the difference between business and personal data?

Under the GDPR, personal data can be defined as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Specifically, data that can be defined as "personal" might be an email address, telephone number, personal documentation number, IP address, etc. In recent years, there has been confusion around whether a corporate email (firstname.lastname@employer.com, for example) is considered as personal data.

Although not directly specified by the ICO, a corporate email address (following the above format) technically falls under the personal data bracket, as it contains data that individualises an identifiable person, regardless of whether it is a corporate email or not. On the other hand, a corporate email that isn't specific to an individual (info@employer.com or contactus@employer.com, for example) is not classified as personal data and therefore doesn't fall under GDPR.

KEY EMPLOYER ACTION

Ensure that your DPO (Data Protection Officer) is aware of the key differences between personal and business data.

3

Do I have to have consent to process personal data?

Under the GDPR, consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Under certain circumstances, however, a business can rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of your organisation's legitimate interests.

The "Legitimate Interests" condition constitutes an added condition for processing data, whereby a business may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The legitimate interests condition has three requirements:

- You need to process the information for the purposes of your legitimate interests of for those of a third party to whom you disclose
- The interests must be balanced against the interests of the individual(s) concerned
- The processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

If a company has processed data on the basis of the "legitimate interests" condition, it must be able to provide a clear assessment of the reasons and evaluation against the interests of the individuals concerned.

KEY EMPLOYER ACTION

The 'Legitimate Interests' condition should only be applied where legally necessary. It is therefore recommended that consent should be sought for processing of ALL personal data.

4

Will the GDPR affect business-to-business (B2B direct marketing (specifically email marketing)?

As explained previously, a corporate email address following a specific format (firstname.lastname@employer.co.uk) is considered as personal data, whereby the first name and last name of the individual is displayed and therefore can be identified. So, as long as a corporate email follows this format, GDPR will apply.

The difference is, however, that the business delivering the communications may argue that it is of legitimate interest to the recipient or the recipients' employer, based on the industry or profession.

For example, a recruitment company sending business information may argue that a hiring manager of an organisation has received communications (before a double opt-in procedure) based on the fact that he or she is currently hiring, and therefore may be of legitimate interest.

An organisation will still need to show that there is a balance of interests and the individuals interests are not out-weighed by the marketing content. Of course, any individual can object to direct marketing and it is one of the examples of legitimate interests for which objection is already fairly well understood and easy to action (often by unsubscribe link or by contacting the company in question to request).

KEY EMPLOYER ACTION

When delivering a B2B marketing campaign using new data, ensure that either consent has been given or the marketing material is directly relevant (industry or role related) to the recipients.

5

Can we still keep our current consumer data and contact them as per usual?

The GDPR brings with it a multitude of data processing changes, including stricter policies on individuals' consent for their data to be processed. Currently, UK businesses that hold data on their customers/consumers will not necessarily have had to implement a double opt-in procedure, as the current data protection law states only a single opt-in is necessary.

This, therefore, suggests that the data is non-GDPR compliant, however, the ICO have said that this may not be the case. Although not confirmed, the ICO have suggested that a business is not necessarily required to 'repaper' or refresh all existing DPA consents in preparation for the GDPR.

But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

In light of this, the ICO does recommend that consent is reconfirmed to ensure that there is no risk when the GDPR is introduced.

KEY EMPLOYER ACTION

To avoid any risk of non-compliance, be sure to prepare a 're-opt-in' campaign to all current database contacts confirming their consent with a simple message and web link asking if they'd like to carry on receiving communica-

6

How long can I store personal data for and where can I store it?

This is one of the most frequently asked questions in relation to GDPR. Whilst there is no specific timeframe as to when you can store data for, the ICO have clarified that personal data should be kept for as minimal time as possible, there are no exact minimums or maximums.

The timeframe should be based on business needs bound against individual rights, for example, in a recruitment perspective, storing a candidate's CV is acceptable until that candidate has made it clear that they no longer require the assistance of a recruitment company, and is therefore granted the 'right to erasure', allowing the individual to request to have personal data erased from the company.

The GDPR states that, unless consent has been given or there is legitimate interest for personal data to be stored for a significant amount of time, the data should be erased when an individuals' rights outweigh the business needs, or in short, is no longer required for business use.

The personal data should be stored with an appropriate level of security, to ensure minimised risk to data breaches. The level of security will differ between data types; however, all personal data should, at least, be kept within a secure folder or programme that is password protected or private.

KEY EMPLOYER ACTION

Confirm an appropriate internal timescale and location for stored data and ensure your employees are aware.

7

Can you monitor/record calls under the GDPR?

Inbound and outbound calls, depending on the content, can still be considered as the transferal or processing of personal data, and therefore falls under the GDPR.

Many UK businesses have a call monitoring policy whereby all inbound and outbound calls may be recorded for training (or something similar) purposes. The ICO has suggested that this activity is GDPR compliant if the recipient has been appropriately notified before the call, either with a pre-recorded or automated message.

The recipient is obliged, under 'the right to erasure', to have the recording deleted only if it has no clear purpose. Most would argue that a phone recording serves a clear purpose with regards to employee training and on boarding, but this can depend entirely on the nature of the business.

KEY EMPLOYER ACTION

It is highly recommended that, if your company phones have the capability to record conversations, there should be an automated message highlighting that calls may be recorded for a specific purpose.

8

What changes are being made to the SAR (Subject Access Request) regime?

Under the DPA, an individual has the right to claim a SAR, which includes the right for an individual to access their personal data so that they are aware of and can verify the lawfulness of the processing. The GDPR brings with it process changes to claiming a SAR, with the most impactful being that organisations can no longer charge a fee for a copy of the information.

Requested information must be provided to the individual within one month of the receipt and include all the personal data that your business holds on that individual.

The SAR, where appropriate, should be provided in an electronic format and the individual making the request should be fully verified using 'reasonable means'.

KEY EMPLOYER ACTION

Ensure your DPO is aware of the new process changes to logging and following-up a SAR.

9

Will the GDPR change a business' social media activities?

Considering the growing popularity of social media, it has become an important marketing tool for targeting specific individuals or groups of individuals. Some platforms, including Facebook and Google, offer a functionality whereby consumers can be targeted based on personal information, such as an IP address or web cookies.

As it stands, there is limited information on whether the GDPR will majorly affect a business' social media activities, however, following the European Commission's proposal for a Regulation on Privacy and Electronic Communications, this could change by the beginning on 2018.

The new ePrivacy directive will enforce stronger privacy rules and may limit certain targeting functionalities on multiple social media platforms. The directive will also cooperate with the GDPR in terms on protection against spam by emails, SMS and automated calling machines. Whilst there is not yet an implementation date for this directive, the ICO has suggested that it may be introduced at the start of 2018.

KEY EMPLOYER ACTION

Keep an eye out for regular updates on the new ePrivacy directive, due to be implemented in early 2018, but not confirmed.

10

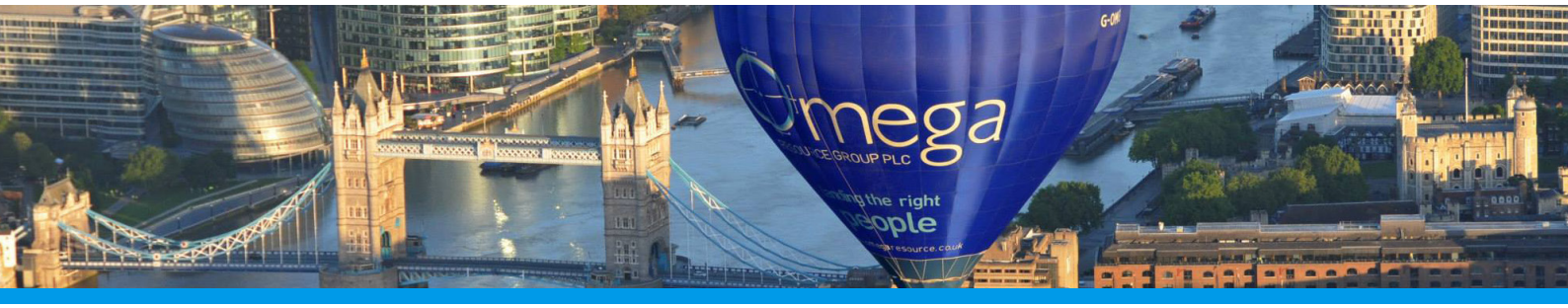
Will I have to seek consent for 'cold calls'?

As mentioned previously, inbound and outbound calls, depending on the content, can be considered as the processing of personal information. In terms of cold-calling or marketing calls, consent is not required as it is considered as business-critical and therefore a 'legitimate interest'.

Live calls can be made to any business number that is not registered on the Telephone Preference Service (TPS) or Corporate TPS (CTPS) or has previously objected to future calls. In practice, this means that live calls should be screened against the TPS and CPTS to ensure GDPR compliance.

KEY EMPLOYER ACTION

Ensure your 'cold call' list has been checked against the TPS and CTPS, as well as those companies that have opted out of your call list previously.



Thank you for taking the time to read our download.

We're always interested in your feedback, so please do get in touch and let us know what you thought of our guide on the GDPR.

T: 01453 827333
M: 07977 516591
E: rachel.harber@omegaresource.co.uk

Omega House,
Bond's Mill,
Stonehouse,
Gloucestershire,
GL10 3RF

Follow me on:

Disclaimer: Omega Resource Group is currently working towards GDPR compliancy in preparation for 25th May. The information published in this download is for guidance only and is based on individual research and brief ICO consultancy. Should you require legal advice on this topic, please contact the ICO on: 0303 123 1113