

Frequently Asked Questions



We recently held a number of seminars on the new General Data Protection Regulations (GDPR) which have been extremely well received.

There were certain questions that came up time and again at each seminar so we thought it may be useful to collate some of the most frequently asked questions from the delegates over all the seminars held and to circulate these.

As we confirmed at the seminars, the answers we have provided are our best opinion in the circumstances given that the GDPR is only in draft form and full guidance has not yet been published by the Information Commissioner's Office. These are by no means definitive answers and are subject to change as we receive further guidance on GDPR.

Question

I have a database which I have built up over a number of years consisting of former clients and contacts, whom I email with new offers or send my newsletter to. Can I continue to email these contacts post 25 May 2018?

Answer

Post 25 May 2018, if you wish to continue to email these contacts you must be able to demonstrate that you have obtained their consent in a GDPR compliant manner, i.e. their consent was freely given, it was specific and informed and the contact gave their consent by taking affirmative, positive action. If you cannot demonstrate this, then if you want to continue to email them, you will need to 'refresh' your consent to be GDPR compliant.

Question

If data is backed up on clouds, servers or other systems which are based abroad then will this constitute an international transfer? For example, if the data is processed in the UK but the company has servers in Brazil.

Answer

Our initial view is that this is likely to constitute an international transfer of data. You should speak to your cloud/server providers and make enquiries as to what security measures they have in place and how they are preparing for the GDPR. You should review your contracts with such providers to ensure that any breaches are notified to you within a short time period (in any event shorter than the time period you will be required to adhere to if you have to notify the Information Commissioner's Office).

Question

If I receive a business card at a marketing meeting, does this constitute personal data under GDPR? Can I add the contact to my database and send them direct marketing information? Do I need to provide the contact with a privacy notice?

Answer

Personal data is 'any information relating to an identified or identifiable natural person' A business card does identify an individual person and so is likely to be captured under the GDPR. However, the fact that the exchange of personal data happens in a business context is significant because the person giving their business card to you will have a reasonable expectation that you will use their details to contact them (including sending direct marketing) for business purposes. You should however ensure in so far as it is possible that the person understands the purpose for which you intend to use the business card by saying something like "Would you like to be included on our mailing list?" Thus in a business to business context you can rely on the legitimate interest ground to send the contact business communications. However, you should still only send marketing to individuals that they would expect to receive and you should always remind individuals of their right to opt out.

Do you still need to provide a privacy notice? Technically yes but in these circumstances you could simply signpost them to your privacy notice when sending your first communication them, either by way of a link in an email or by including a copy of the notice if communicating by post.

Question

I keep client/contact details in case the client/contact comes back in the future. Is that ok?

Answer

Under the GDPR data must only be kept for as long as is necessary. Therefore, once the data becomes obsolete or unnecessary for the purposes you originally obtained it for then this data should be permanently deleted (including off all electronic systems). One of the main exceptions to this is when you have a requirement under law to retain this information, for example as dictated by HM Revenue and Customs. You could keep this information if you have obtained consent to retain it for a specific length of time provided that you specify the reasons and length of time for which you are retaining it and how you have determined that length of time to be appropriate. For example, as a law firm we keep client records for a period of 6 years. This is not a legal requirement but the limitation period is 6 years so we choose to keep the records for this period in case of a claim being submitted within this period. Of course you must ensure the data is deleted if consent is not provided, if consent is withdrawn or once the agreed time period has lapsed.

There currently has been no further guidance issued by the Information Commissioner's Office but we will continue to keep an eye on this. There is however a useful tool available on the website whereby SME's can carry out a self-assessment. Some of you may find this useful and it will expand further on the 'steps to take now' section of our presentation. This is available at: <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>

We are in the process of reviewing Terms and Conditions, contracts with third parties (including those which govern the relationship between Data Controllers and Data Processors), staff / employee handbooks and contracts of employment on behalf of clients. We can also create a template Privacy Notice / Data Information Sheet which will outline the information you must provide to a data subject under the GDPR and tailor this to your business. Should you need any assistance then please do let us know as soon as possible to discuss how we may be able to assist.

We will be sending out further updates as further guidance is published, should you wish to receive such updates then please inform us by way of reply. Please note that this will be separate to our firm wide marketing list and you will only be e-mailed GDPR updates (unless of course you have signed up to our general marketing list previously).