DATACONVERSION

YOUR GUIDE TO DATA BREACHES UNDER GDPR

hello@dataconversion.ie | www.dataconversion.ie| +353 1 804 1298

DATACONVERSION

So we have talked a lot about what to do to prevent a potential data breach. However, although you may take every step necessary to mitigate risk, breaches are unfortunately, never 100% preventable.

Many companies such as Uber and Hilton Hotels have fallen victim to hackers over the past few years. These hackers launch malicious cyber-attacks in which they attempt to extract sensitive data such as customer usernames, passwords and bank details etc.

And cyber-attacks aren't the only thing you have to worry about. Personal data can just as easily get into the wrong hands or be made publicly available through human error. If this does happen, the question then becomes how to correctly respond under GDPR.

Hopefully we will be able to give you a brief understanding of what is expected of you throughout this post.

The GDPR comes into effect on the 25th of May 2018 and will affect all companies who conduct business within the EU. This of course does not mean that it will solely impact EU member states. It will impact any company that has customers or clients etc within the EU even if the company physically sits outside of the EU.

The GDPR is solely focused on the protection of Personal Data of EU citizens and people living within the EU and seeks to implement new regulation to better protect it. They will be enforcing these regulations with a strong hand.

Companies found in breach after the May deadline may be subject to fines of up to €20 million or 4% of global turnover, whichever is greatest.

DATACONVERSION

WHAT IS A PERSONAL DATA BREACH?

According to the GDPR a personal data breach is considered to be;

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored, or otherwise processed".

An example of a Personal Data Breach could include an instancein which a device containing a copy or a partial copy of a controller's database has been lost or stolen. For example a USB key containing a customer list being lost in transfer or something as simple as a practitioner misplacing a briefcase containing client information.

The GDPR introduces the requirement for a personal data breach to be notified to the competent national supervisory authority (in Ireland, this is the Office of the Data Protection Commissioner). In certain cases it will even be necessary to communicate said the breach to those individuals whose personal data may have been affected.

Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach. This in turn allows individuals involved to take the steps necessary to protect themselves from its potential consequences.

Some EU states may have an existing breach notification obligation in place, Germany for example. Certain organisations will also already be familiar with such requirements, such as providers of publicly-available electronic communications services.

DATACONVERSION

TYPES OF DATA BREACHES

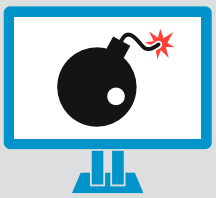
According to WP29 data breaches can be categorised into one of the following;

Confidentiality Breach

Where there is an unauthorised or accidental disclosure of, or access to, personal data.

Integrity Breach

Where there is an unauthorised or accidental alteration of personal data.



Availability Breach

Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Of course given the situation a breach could concern all three of the above.

In a situation whereby an individual's personal data is temporarily unavailable due to a security incident the lack of access to the data could have a significant impact on the rights and freedoms of the individual. It is therefore considered to be a breach. If it is unlikely to cause any harm then it may be exempt.

For example your company's systems being unavailable for several hours resulting in you being unable to send newsletters to subscribers. In addition, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security'.

DATACONVERSION

WHAT HAPPENS IN THE CASE OF A BREACH?

Now let's get down to the nitty gritty. What can you expect to go down if you are found in breach? First and foremost notification is mandatory unless a breach is unlikely to result in a risk to the rights and freedoms of individuals as noted above. We would therefore encourage you to plan in advance. Putting relevant processes and procedures in place to detect and contain a breach.
Processes should also be in place to assess the potential risk to individuals, and subsequently determine if it is necessary to notify the relevant supervisory authority. Additionally you may be required to communicate the breach to the individuals concerned with the breach.

The GDPR contains provisions on when a breach needs to be notified (see below), and to whom, as well as the information to be provided and as such we would recommend consulting this for further information.

Depending on how severe the breach is, and more importantly the personal data obtained, the impact to the individual could be highly detrimental.

For example the recent breach faced by the smartphone manufacturer OnePlus who recently faced a breach which resulted in customers' credit card information being stolen while they were purchasing OnePlus products from their online store.

Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals8, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary.

DATACONVERSION

WHEN TO NOTIFY?

In the case of a personal data breach, it is essential that it is reported by you, the controller, to the relevant supervisory authority within 72 hours (i.e. the Office of the Data Protection Commissioner. Now, to confirm, this means 72 hours from when you become "aware" of the breach not necessarily 72 hours from when it occurs. In a situation where the notification to the supervisory authority is not made within 72 hours, you must ensure you provide reasons for the delay.

Of course you may not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it. If you find yourself in this situation then don't panic, the GDPR has taken this into consideration and as such, it allows for a notification in phases. If this happens you should inform the supervisory authority of the fact that you do not yet have all the required information and will provide more details later on.

So when exactly will you, as a controller, be considered to be 'aware'? Well according to WP29 this occurs once you have a reasonable degree of certainty that a breach has occurred that has led to personal data becoming compromised. Take for example if you were to lose a USB key which contained unencrypted personal data it is likely to be difficult to determine whether or not the data has been accessed by unauthorised personal. Regardless this would have to be notified as there is a reasonable degree of certainty that an availability breach has taken place. Here you would be considered to be aware once you realised that the USB key had been lost.

Once you, as a controller have become aware of a breach you should assess the likely risk to individuals in order to determine the action(s) needed to address the breach. Having the necessary processes in place to be able to detect and address a breach are therefore essential. The focus of any breach response plan should be on protecting individuals and their personal data.

DATACONVERSION

WHAT INFO IS TO BE PROVIDED?

When it comes to notifying a breach some basic information should be provided. This has been outlined in Article 33(3) which states that the breach notification should include the following;

"(a) a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) The name and contact details of the data protection officer or other contact point where more information can be obtained regarding the breach;

(c) a description of the likely consequences of the personal data breach;

(d) a description of the measures taken or proposed to be taken by the controller to address the personal data.

breach, including, where appropriate, measures to mitigate its possible adverse effects."

So there you have it, almost everything you need to know about a breach under GDPR! For further information/ assistance on any of your GDPR related queries be sure to contact us today on +353 1 804 1298.

www.dataconversion.ie

+353 1 804 1298

hello@dataconversion.ie

Dataconversion
25-26 Westland Square
Pearse Street,
Dublin 2
D02 N403