Dat tes

Introduction

As thorough as your efforts to pro be, there is still the potential for a personal data breach to occur.

Personal data breaches can be . A personal data breach is any breach of security which results awful destruction, loss, alteration, unauthorised disclosure of, or acc

A commonly-reported example of h is the loss of mobile computing devices containing work-related p aving the company laptop on the train' trick). Another example, perh , is unauthorised access by a third party, usually referred to as ha can include accidentally sending personal data to the wrong recipie l data without consent.

Some, but not all, personal be reported to the Information Commissioner's Office ("ICO"). S so be reported to individual data subjects themselves. Strict time li notification obligations. As soon as you become aware of a data b ess, therefore, it is important to establish whether it needs to be re

Part 1. Recognising a Per n

In many cases, it may be obvious ach has occurred. In other cases, however, more examination may rs can help focus your analysis of an incident:

a) **Confidentiality:** C compromised in cases where personal data has unauthorised recipient. This can happen deliberately

b) **Integrity:** Integrity personal data is altered without authorisation. Agair rately or by accident.

c) **Availability:** This authorised availability and non-availability. On the access may occur; on the other hand, access to pe for example, when data is deleted or otherwise destr ilability can be compromised on purpose or accident

Examples of data breaches might

- The loss or theft of a physi
- The loss or theft of compu a laptop or smartphone, portable data storage, for example a storage devices;
- Equipment failure;
- Unauthorised access to, of personal data (or inadequate access controls allowing su use, or modification);
- Human error (e.g. sending ng recipient);
- Unforeseen circumstances d
- Hacking, phishing, and oth whereby information is obtained by deception.

Different members of staff within different levels of knowledge and training concerning data protectio re, that anyone handling personal data has at least a basic understa to recognise the signs of a data breach, even if they do not have t and skills to handle that breach in full.

Internal procedures within your b what your staff should do if they discover or suspect a breach. Du apply to your reporting obligations under the UK GDPR, it is importa quisite knowledge and authority to handle the breach (for example, y er ("DPO") are informed quickly.

Data Processors

An important point to note at this s rocessors. A data processor is an individual or organisation who pro your behalf (in your capacity as a data controller).

If a processor suffers a persona lves personal data that they are processing for you, they must inf delay" as soon as they become aware of it. It will then be up to y notify the ICO and affected data subjects, if the risks and conseque ation.

Part 2. Assessing Risk &

The focus of the UK GDPR is on freedoms of individuals. It is, after all, their personal data that you a s when investigating an actual or suspected personal data breach, ed to those rights and freedoms. If such a risk is likely, the ICO must h. If not, you do not have to report the breach to the ICO. Even if yo not necessary to report a breach, however, it is important to keep ir and governance principles of the UK GDPR. Any decision like thi d, along with the reasoning and justification.

Is There a Risk?

This, then, is the key question wh ckly if you are to comply with your obligation to report a breach to t e – within 72 hours of becoming aware of it.

At the heart of the risk are the equences for the individual data subject(s) whose personal data As Recital 85 of the UK GDPR states:

> *"A personal data breach an appropriate and timely manner, result in physical, damage to natural persons such as loss of control ov or limitation of their rights, discrimination, identity the , unauthorised reversal of pseudonymisation, damag confidentiality of personal data protected by profess er significant economic or social disadvantage to the d."*

In short, the negative consequer g. Sometimes, the only real risk stemming from a data breach will hose that use the personal data in question in their line of work. On t aches can result in very real harm to individuals. Emotional distress, ms of material damage, and even physical harm can sometimes ste breach. Your evaluation of these risks, therefore, must not be taken

When assessing risk, two aspects the likelihood and the severity. As guidance from the EU's Article 2 replaced by the European Data Protection Board) explains, you a pothetical event as you would be when conducting a Data Protectio u are looking at an event that has actually occurred and focusing f the impact of that breach on individuals.

The Article 29 Working Party Gui king at several factors that should be considered when assessing ri nsidered in combination with one another, not just separately:

- The type of breach that has
- The nature, sensitivity, and involved;
- The ease of identification o ;
- The severity of the conseq s involved;

[1] As of 1 January 2021, the EU GDPR the UK GDPR. We consider that the European Data Protection Board's g ever. These Guidance Notes will be updated as the ICO issues new UK-ce the future.

- Any special characteristics ;
- Any special characteristics . your business); and
- The number of affected ind

Each of these points will now be nore detail. As noted above, it is important to remember that in mar aspects will overlap and should be considered in the round, not in iso that there is no risk on one basis, but another basis may highlight a s

The Type of Breach

This directly relates to the s d the level of risk. A breach in which confidential inform d to an unauthorised third-party will have different c ndividuals concerned to a breach in which that inform cannot be recovered.

The Nature, Sensitivity, a Data

Generally speaking, the m e greater the risk of harm. There are, however, additio mportant to remember that personal data involved in ned with other data about someone. A name and adc likely result in a great deal of harm; however, if that is a, the risk may increase.

Taking, for example, identi t information, these can all cause harm by themselves combination, however, the risk of identity theft arises ore potential harm for the individual data subject.

It is also important to t which may appear quite harmless. Could that data s purposes? Of particular interest is the Article 29 le of a list of customers receiving regular deliverie own, such data is quite inconsequential from a da If that data also revealed customers whose deliveri for a holiday, however, it would suddenly become qu s.

Ease of Identification

Given that the protection important question is how easily they can be identifi ed in the breach. In some cases, this will be obvious directly identify people. In other cases, however, the s traightforward.

Personal data may have b ast pseudonymised. If this is the only data involved in hould not be automatically assumed that there is no to consider whether such data can be combined er to identify individuals. Answering this question wi on of the availability (public or otherwise) of related per

This point in particular a e the importance of data security measures. Pseud useful, but in isolation this may not be sufficient. Ad as strong data encryption should be considered and ossible, thereby making it

much harder to read (and ople) any data without the decryption key (which, it go d be closely guarded).

Severity of Consequence

This connects to the type each. As noted above, the more sensitive the data in e greater the risk of harm. The permanence of the p should be considered. The longer the affected data su pacted, the higher the risk factor.

It is also important to consi has obtained the personal data in question. If data ha y sent to the wrong person or organisation, but that pa ur business already has an established relationship, th y be trusted to act on your instructions to delete or re se it. In this scenario there has still been a breach, but duals stemming from it will be low to nil, meaning that still be recorded internally, you may not need to report r factors).

Special Characteristics o

The risks posed by a data the personal data involved relates to children or to ot s as they may be put at a greater risk of danger as a

Special Characteristics o

The nature of your busines ay also have an impact on the level of risk since it wi determine the type of data you use and what you use

This generally ties in direct the personal data involved. A mailing list for a newsle s risky as special category personal data (formerly kno al data") relating to medical conditions.

The Number of Affected I

This point follows on natu oint in that, depending on the nature of your busines l data relating to a smaller or larger number of peop more people involved, the greater the risk; however, ed that a small number (or even a single individual) m other points set out above should still be considered small the number of data subjects involved in the bre

Time Limits

As noted above, if your risk asses ta breach indicates that there is a risk to the rights and freedoms of ersonal data is involved, you must inform the ICO within 72 hours of k each.

This is not a time limit that is set i it particularly flexible. If there is a delay, you must explain it. It is, the k to the 72 hours if you can.

The time limit is made easier to … the fact that you do not have to provide full details to the ICO in th… rly in more complicated cases, 72 hours may not be long enough to … and assess what action needs to be taken. You are, therefore, able … the ICO in phases, so long as you do this without further delay. Furth… s:

> *"If you know you won't be… ails within 72 hours, it is a good idea to explain the … hen you expect to submit more information."*

What to Tell the ICO

The UK GDPR requires that, wher… ta breach, you provide *at least* the following information to the ICO:

a) describe the nature… each including where possible, the categories and ap… ata subjects concerned and the categories and appr… onal data records concerned;

b) communicate the n… s of the data protection officer or other contact point … can be obtained;

c) describe the likely c… onal data breach;

d) describe the meas… to be taken by the controller to address the person… , where appropriate, measures to mitigate its possible…

How to Tell the ICO

The ICO provides a breach report… vailable here. The same page also provides a self-assessment tool … nen determining whether or not a breach is severe enough to report.

Part 3. Notifying Individu

Looking back at the risk assessm al data breach presents not just a risk, but a *high risk* to the rights ual data subjects, the UK GDPR requires you to inform the individu ossible.

In short, this means that if the breach on data subjects is more serious, and/or the likelihood of t ass is higher, then individuals will need to be informed, particularl ll need to take steps to protect themselves.

It is also important to remember that it is not necessary to notify individual data subjects, you may ICO, depending on the level and severity of risk. Once again, recor tant, and you must document your decision-making and justifications ify.

Time Limits

The requirement to notify individua uirement to notify the ICO. Rather than setting a fixed 72-hour limi only that you should inform data subjects "without undue delay". In as you can. Failure to inform data subjects promptly is only likely to of the potential consequences for them.

What to Tell Data Subjects

The emphasis here is on clear and portant to remember that individual data subjects will most likely not b tion, lawyers, or even familiar with *business-speak*.

At a minimum, you must provide th

- the name and contact de tion officer or other contact point where more information ca
- a description of the likely c onal data breach; and
- a description of the meas to be taken by you as the data controller to address the b appropriate, measures to mitigate its possible adverse effects

Exceptions

There are some limited circums UK GDPR which may justify not informing individual data subjects n:

a) the controller (i.e nted appropriate technical and organisational prote se measures were applied to the personal data affec a breach, in particular those that render the persona y person who is not authorised to access it, such as e

b) the controller has ta es which ensure that the high risk to the rights and fre ...is no longer likely to materialise; or

c) it would involve disp ch a case, there shall instead be a

public communicat whereby the data subjects are informed in an equa

The final point in particular must b ception to informing data subjects, only an exception to informing the

How to Tell Data Subjects

The third exception above notw rable to use dedicated personal messages whenever possible. Su specific and should not attempt to bury the information about the ation such as news updates or marketing messages.

Direct messaging such as email, nly-used messaging services are among the easiest ways to notify ent banners on your website may also be acceptable according to g 29 Working Party. Non-electronic methods include notification by po sements in print media.

Under the heading of “what not t sense. Press releases, corporate blogs, and other methods of co ted audience that is not likely to consist of many data subjects, will

Part 4. What's Next?

Whether notification is required o record-keeping and accountability remains. If a personal data breach business, it must be documented. When recording a personal data b quires that you document both the facts relating to the breach itself a ken.

Not only is this important from a c that it makes it possible for you to demonstrate your compliance with ICO. There is, however, a bigger picture, and that is the importance as a learning exercise.

Whether the personal data breach ate, your investigation of it should help to highlight solutions which ry least help to prevent) a repeat performance. The need for more ing for your staff may be shown, processes may need to be imp ore secure technologies may be required, and so on.

A personal data breach may in eff en, for a comprehensive review or audit of your business's collection, onal data. Consider, for example:

- Your existing method(s) of
- Where and how personal d
- Your current organisationa y measures for the protection of personal data along with th knesses of such measures;
- Your existing policies and personal data and for dealing with events such as breaches;
- The methods used for tra both electronic and physical, and whether or not those meth
- The level of personal data between your business and third-parties (whether they are) and whether or not that level is necessary;
- Whether any data protecti eed to be conducted for upcoming projects and whether asse out for existing uses of personal data need to be reviewed;
- Raising awareness of pe among staff, with training where appropriate.

There is no doubt that personal d upsides for anyone involved. Not only are there often significant r data subjects, but also to your business. A loss of trust and tation can be extremely costly. Furthermore, if you fail to notify a l tances require that you do so, you may face a fine of up to £8.7m or 2 r.

A proactive approach to data pro on of data breaches is essential. Regular audits will help to ensure age, and use of personal data, as well as the framework within your , stays up-to-date and in line with prevailing best practice, not to me v. When considering new uses for personal data, in particular where olved, it may be advisable or even legally required to conduct a data ssment. Awareness is key, and a data protection by design approa can help prevent the worst from happening. If it does, however, t earn, improve, and ensure that it doesn't happen again!