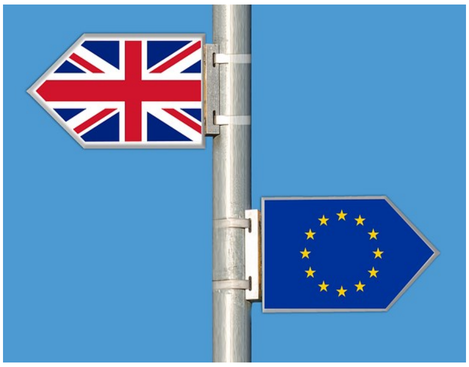
DATA PROTECTION NEWSLETTER

JULY 2016

BREXIT—WHAT NEXT FOR DATA PROTECTION?



You may think that the UK leaving the EU means that the new General Data Protection Regulation will no longer be relevant in the UK. This is not necessarily the case.

If the UK remains part of the European Economic Area the regulation will still apply. If not, to share data with any businesses or institutions in the EU, or to process the data of EU citizens, the UK will need to prove that appropriate measures are in place to protect personal data. In any event, if the UK is still a member of the EU when the regulation comes into force in May 2018, we will have to adopt it by this deadline. This article sums up why we can't ignore the GDPR.

As developments progress in these uncertain times, we will keep you informed. Read the ICO's latest press release and blog post about the future of data protection.

PRIVACY SHIELD UPDATE

Under current UK Data Protection Law, information should not be shared with countries outside the EEA unless they can prove they have adequate protection for personal data. This will not change unless a new law is passed. Therefore the UK should still use EU guidance when transferring personal data to the US. The European Commission has made amendments to the EU-US Privacy Shield agreements. The were approved last week and Privacy Shield is now in place. However there are still concerns and Data Protection specialists predict the Shield will soon be challenged. If you have any queries about transferring personal data to the US, please email us.

DP AUDIT 2016

We will soon be sending out this year's data protection audit. If you are a DP contact please look out for your form. You can find out more about the audit on our SharePoint page. If you have any questions about this, please contact us.

DATA PROTECTION TRAINING

To help prepare for the future, whether it be UK law or GDPR, the ICO advises that everyone ensures they are meeting best practices under the current legislation. Remind yourself of what you should be doing by completing the online Data Protection Training Module.

NEWS

- Names and dates of birth of NI prison officers sent to contractor in a spreadsheet
- Location based fitness apps break Data Protection law
- California Court House makes defendant’s database available to public in error
- Smart TVs are listening to us and sharing sensitive personal data without our knowledge
- University of Greenwich suffers ‘revenge hack’ by former student who posts staff and student personal information online.
- Liverpool John Moore University accidently sends staff tax details to ex-employee.
- Police officer sentenced for sending a relative the personal details of witness
- US county mental health department suffers breach when report left behind during office move.

- **Watch out for imposters.** In our last newsletter we highlighted the threat of email phishing scams. But you should also be aware of scams via the phone. Don’t give out personal information unless you are sure who you are talking to.
- **Get rid of data you no longer need.** Regularly review the information you hold and decide whether you need to keep it. If the data is not held it cannot be lost, stolen or inappropriately accessed.
- **Avoid creating unnecessary copies.** Secondary copies are more likely to be lost and cause a data breach. Copies also tend not to be kept up to date—breaking the 4th Data Protection Principle.

WHAT IS A DATA BREACH?

A Data Breach is when data is viewed or potentially viewed by someone who should not be able to view it. This could be someone external or staff who should not have access to the information. A data breach could involve any information. A breach only breaks Data Protection legislation when it contains personal data relating to living individuals.

Data breaches are not only caused by high profile hacks. In fact, human error is the most common cause of data breaches. This could be as simple as leaving personal data at a printer or leaving a file unsupervised. A data breach could involve sending an email containing personal data to the wrong person or losing an unencrypted USB stick.

A recent string of data breaches at a council in England, show how small breaches can add up.

The University of Greenwich recently suffered a breach after student information was posted online. At University of Oxford a member of staff emailed exam results, including those who had failed, to all students on the course.

To make sure you protect against a breach you should think about:

- **How you store personal data**
- **How you use personal data**
- **Who you share personal data with**
- **How you send personal data**
- **Who should be able to access personal data.**
- **How long you retain personal data for.**

Each area should have in place measures to keep personal data secure. Look at our Sharepoint pages to find out how to handle personal data. You can also find out what to do if there is a data breach.