ARE YOU READY FOR GDPR? WHITEPAPER

BRIGHTERDIRECTIONS.CO.UK

GDPR stands for General Data Protection regulations, which is being put into place on 25th of May 2018. Even with the UK's decision to leave the EU, the government has confirmed that it will not affect to commencement of the GDPR.

The GDPR is put in place to outline what companies can and can't with regards to processing personal data. Every organisation will have to comply with the new law, but not every business will need to appoint a Data Protection Officer. All organisations who deal with businesses within the EU must comply with the GDPR.

Who will need to appoint a Data Protection Officer?

1) Public authorities
2) Organisations that engage in large scale systematic monitoring - FOR EXAMPLE / ADD MORE SPECIFIC INFO ON WHO IT AFFECTS
3) Or organisations that engage in large scales of processing personal data

If your organisations doesn't fall into any of the above, then you don't need to appoint a Data Protection Officer although you MUST appoint a DPO if your organisation DOES fall in to one of the above categories.

With regards to what 'large scale' constitutes, the EU has no specific figure or definition but a guideline instead for organisations;

It is not possible to give the exact number with regards to;
1) The number of individuals concerned
2) The amount of data being processed

It is recommended that below factors are to be considered when determining whether the processing of data is being carried out on a 'large scale';

1) The geographical extent of the processing activity
2) The permanence, the duration of the data processing activity
3) The number of data subjects concerned - either as a specific number, or as a proportion of the relevant population
4) The volume of data, or the rang of different data being processed

Examples that do not contribute to large-scale processing include;

1) Processes of personal data contributing to criminal convictions or offences by an individual lawyer
2) Processes of patient data by an individual physician

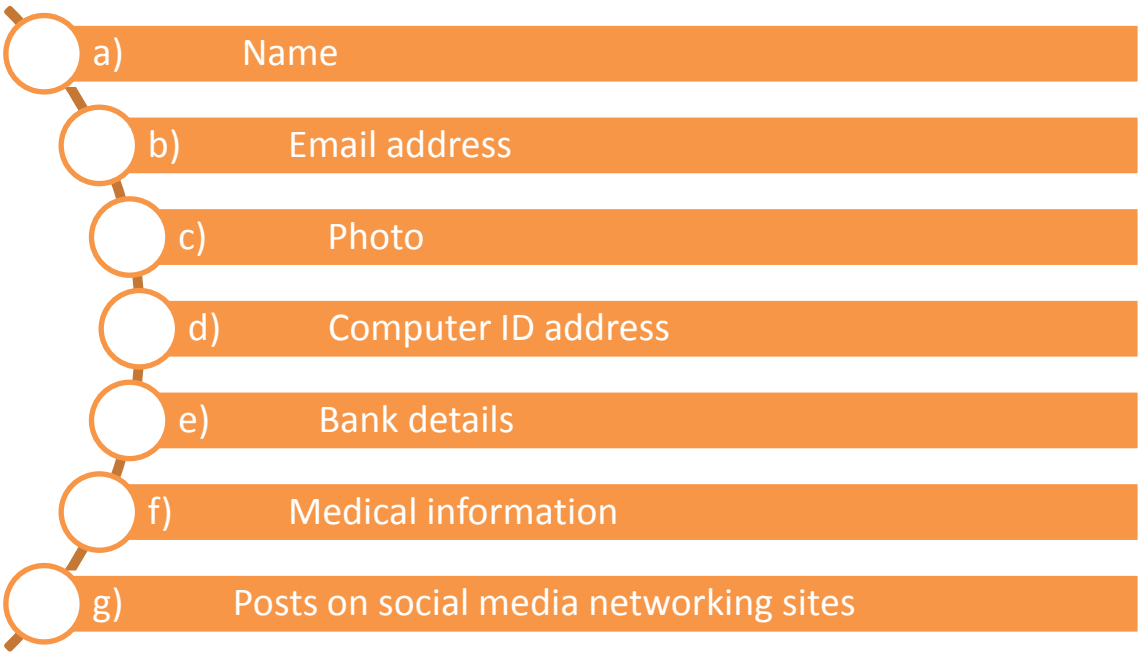
An example of large-scale processing includes;

1) Processing of data by telephone, or internet service provides
2) Processing of customer data in the regular course of business, by insurance companies or banks.
3) Processing of personal data for behavioural advertising by search engines
4) Processing of patient data in the regular course of business by a hospital
5) Processing of travel data of individuals using a city's transport system

What constitutes personal data?

Any information related to a data subject or natural person, which can either be used directly or indirectly to identify a person.

Below are a few examples of personal data;



Expectations of the GDPR;

1) If your organisation does not have a structured filing system according to specific criteria, then those files should not fall within the scope of the regulations
2) The regulation does not apply if the processing of personal data is used specifically for personal or household activity with no connection to professional or commercial activity.
3) The regulation does not exclude Member State Law that sets out the circumstances for specific processing systems; this is including determining more precise conditions under which the processing of personal data is lawful.

The GDPR will provide data rights (8 in total) to all EU residents concerning their personal data such as;

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Personal data should be;

- Processed in an appropriate manner to maintain security
- Retained only for as long as necessary
- Accurate and kept up to date
- Adequate, relevant and limited to what is necessary
- Collected for specific, explicit and legitimate purposes
- Processed lawfully, fairly and in a transparent manner

Consent to personal data must represent a 'freely given, specific, informed and unambiguous indication of the individuals wishes'. The regulation imposes stricter requirements on obtaining valid consent from individuals to justify the processing of their personal data. Organisations are required to keep records so that they can demonstrate that consent has been given by the relevant individual and cannot count silence, pre-ticked boxes or inactivity as consent.

One of the key aims of the GDPR is to empower individuals and allow them control over their personal data. While the regulation is in place to largely preserve the existing right of individuals to access their own personal data, it also confers significant additional new rights of individuals. New data access rights:

a) 'The right of erasure or right to be forgotten'
b) 'The right to data portability'

All data must be provided for free, in an easily accessible and structured form and within one month of a request. The deadline can be extended to three months, if the request is complex.

GDPR will provide EU residents rights to allow them to learn about how their personal data is handled and to be able to identify any issues or concerns with the way it has been processed.

a) 'The right to be informed'
b) 'The right of access'
c) 'Rights in relation to automated decision making and profiling'

Companies shall be held to account over automated decisions regarding personal data and must ensure that all individuals affected can obtain human interventions, an explanation of the decision and the opportunity to challenge it.

GDPR provides means through which individuals can request that their information is to be corrected, or that no further processing of their personal data is to be carried out.

a) 'The right of rectification'
b) 'The right to object'
c) 'The right to restrict processing'

Organisations may be required to restrict processing if a data subject contests the accuracy of the data held which concerns them, or if they have raised any objections to it being processed.

Penalties and Fines under the GDPR regulations

The NEW regulation comes with heftier fines and harsher penalties if organisations do not comply with GDPR. *GDPR templates are available on the web & ICO net, RSA web (white papers)*

Penalties

- You can be fined up to 20 million for a data breach
- 4% of the annual turnover of a company
- Before the 4% penalty, they can warn you in multiple ways
- Art 82 (1) GDPR – allows anyone who has their data breached the ability to sue. Whether or not the damage done is materialistic or not
- Art 25 GDPR – Unnecessary data is a liability
- Art 35 GDPR – Read this section

Legal GDPR

- Breaches
- Fines
- Sanctions

Breaches

- Security of data, leading to accidental or unlawful destruction, loss alteration, authorisation, disclosure of, or access to personal data transmitted, stored or otherwise processed
- Confidentiality breach
- Availability breach
- Integrity breach

RSM – Case Study

GDPR case study: government

RSM firm: Netherlands
RSM contact: Rien Hommes & Gerrit Goud

BRINGING RSM'S IDEAS AND INSIGHT – THE WORK WE CARRIED OUT

We implemented a privacy control framework using an Information Security Management System from Key 2 Control, a software company associated with RSM Netherlands. The system enables the local government and its internal audit department to control and document data security and privacy policies and procedures within the government organisation.

The approach is focused on the PDCA (plan-do-check-act) cycle with attention to risk management, in line with the GDPR. There is a strong focus on control of the privacy processes and the persons responsible for privacy management.

UNDERSTANDING OUR CLIENT – THE BENEFITS

The end result is a privacy management system (PMS), based on the PDCA-cycle. The system is based on the GDPR as control framework. Using this PMS, the organisation can demonstrate the operational effectiveness of their processes, as these are documented in the system together with the related policies and procedures.

By using this system, the quality of privacy management is enhanced at reduced costs.

ARE YOU READY FOR GDPR? WHITEPAPER

BRIGHTERDIRECTIONS.CO.UK

Bell Educational Services LTD case study

IT Governance

Specialist services and solutions for IT governance, risk management, compliance and information security.

Case Study

Bell Educational Services Ltd implements data protection privacy framework on advice from IT Governance's expert consultants

Bell Educational Services Ltd contacted IT Governance to obtain advice and project support from our experienced data protection consultants. Bell's management team wanted to know the exact standing of the organisation's legal situation, security practices and operating procedures in relation to the Data Protection Act.

Management Systems consultants Ralph O'Brien and Nick Orchiston and qualified DPA auditor Richard Campo from IT Governance enabled the company to achieve its compliance goals and helped the organisation to plan and implement best practice measures to protect confidential data at all points in their system.

BACKGROUND

For more than 60 years Bell has carried out English language teaching activities around the world as an educational charity, becoming one of the leading providers of language education in Britain. Over the last ten years more than 100,000 students from over 90 countries have studied English with Bell in the UK alone. This sizeable business operation has generated large stores of data, much of which is personally identifiable and confidential.

At the beginning of 2012 the Senior Management Team at Bell decided to review its Data Protection Act compliance and carried out a risk assessment that looked at the threats to confidential data stored within the organisation. To establish what corrective actions would be necessary to address areas of risk, Bell called in a DPA consultant from IT Governance.

REQUIREMENTS

The main drivers for this compliance project were:

1) compliance with the UK Data Protection Act 1998;
2) protection of personal/sensitive information regarding Bell students; and
3) prevention of data breaches that could lead to loss of reputation.

ARE YOU READY FOR GDPR? WHITEPAPER

BRIGHTERDIRECTIONS.CO.UK

Gordon Sinclair, the Deputy IT Manager and IT Project Manager, described the project requirements below:

"Bell wanted to take appropriate steps to ensure that confidential data was being handled in accordance with UK law and also that sufficient safeguards were in place to secure that data in line with the risk appetite of our business. Caring for our students includes protecting their personal data, and our reputation in the education and training market was only one of several good reasons for ensuring that we were compliant. This meant that we needed to assess how we handled our data to ensure that we had all the appropriate security controls in place to provide the highest level of protection at all times.

We hired IT Governance Ltd's experts to assess our data protection arrangements, identifying what constituted information protected by the Data Protection Act in our system, the activities regulated by the Data Protection Act designed to protect this data, the various rights and obligations under the Data Protection Act, who was responsible for the "purpose and manner" of processing and what the Law requires, and how long data protection rights and duties would last in relation to the confidential data held.

When Bell commenced this project in 2012 we wanted experienced data protection consultants to assess the exact standing of our legal situation, security practices and operating procedures in relation to DPA compliance. This covered everything from storage of student records, how we handled credit card data, what information was held, our retention guidelines (i.e. what we actually needed to retain and for how long), and data workflows to the methods used to move data around, including paper-based records."

PROCESS

Gordon Sinclair explained the process:

"We began with a gap analysis performed by IT Governance's Ralph O'Brien, who identified where we needed to enhance controls to data handling. The work extended to Ralph's recommending tougher security measures and helping us to migrate our manual systems to electronic data handling.

One of the key challenges that we found when attempting to implement privacy compliance was that of trying to establish a set of meaningful guidelines or a recognised standard against which to work. Standards are an increasingly important requirement in governance frameworks: we need a standards-based approach to understand what needs to be achieved; to set common governance goals across and between organisations; to understand whether the responsible managers are competent to implement those controls; and to audit whether those controls have been properly established and maintained. On the advice provided to us by IT Governance we decided to align our privacy framework at Bell against BS10012 - Data Protection - Specification for a personal information management system (PIMS).

The core of our data handling is our registration process, which we are gradually migrating to our CRM system. We are moving information to a secure system based on Active Directory with robust IT security

controls such as regular AV scanning, gateway monitoring and a full set of security policies (45 in total). Management Systems consultant Nick Orchiston showed us how to interpret what we were already doing in this regard into further documents that would support our data security. With his help, we also instituted training 'drop-ins' for staff handling confidential data to enable them to apply the new policies effectively. Perhaps one of the most useful aspects of IT Governance's advice, though, came in terms of senior management team buy-in to the ideas that Nick put forward. As an IT department, we were able to make faster progress with the DPA project thanks to Nick's knowledge and understanding. It was decided that we appoint a member of the Risk Committee as a Data Protection Officer (DPO) as part of their contractual responsibility, which assisted us in configuring the data protection structure to complement our current risk register. It's a decision that we have valued ever since because we have been able to embed DPA awareness and compliance throughout Bell. It's even part of everyone's terms of employment when they join the organisation and forms part of their induction – something that Nick suggested. Data security is considered as important as any other senior management responsibility, and is delegated to all our departments. The idea of trying to implement effective DPA compliance without this senior level of buy-in and integration of the data protection culture into everyday working practice would have been a struggle for us in the IT department.

I would recommend anyone in our situation to hire a consultant like Nick, who has senior management experience from a long career, and of course I would also point you in the direction of IT Governance Ltd!

We had complete confidence that the law's requirements were being interpreted with clarity and that the output would be robust."

OUTCOME

Gordon Sinclair summarised the outcome of the project like that:

"Before completing this phase of our DPA compliance project, we wanted a thorough external audit of our information security and data protection processes and documented procedures. We invited IT Governance to conduct this and Richard Campo carried out the work. Richard proved to be a highly effective auditor and his guidance on our implementation of data protection processes was enlightening. Not surprisingly, he had a high level of awareness about the requirements of the DPA and how the processes that we were operating could be beefed up to further strengthen our stance. The results of this audit performed in 2013 satisfied our Risk Committee that, as an organisation and in terms of the commitment of our individual staff members, we had performed due diligence and that we were fully compliant in terms of UK law. As you can imagine, since we are a respected educational establishment that is among the best in the world, we mark our own efforts strictly so I have a high level of confidence in the outcomes.

For me, the interesting by-product of greater efficiency was a particular plus point in this project. The move from more traditional processes that were admin-heavy to an IT-based system throughout has been especially satisfying, proving the value of IT investment. We now have the ability to get into the system from anywhere in the

ARE YOU READY FOR GDPR? WHITEPAPER

BRIGHTERDIRECTIONS.CO.UK

BD process for GDPR regulation

Brighter Directions as an award winning SME Digital Marketing Company, have also had to go through the processes to comply with GDPR regulation. We want to share with you in a quick bullet point form below and hopefully give you some insights on how we cleansed all our data to comply with the new law.

- Identifying the data
- How you obtained the data
- How you will start to process the data
- Cleanse all current data – (Plan how you intent to do this)
- Continue your method which best works for you organisation
- Plan out how you intend to keep managing your data

GDPR will apply to any company that handles personal data, whether these are corporate businesses or SME's. As above you will need to comply regarding storage of data, secure collection of data and the use of personal information. Although there is a positive side to being an SME, GDPR recognises that smaller businesses will clearly require different processes to what larger or public enterprise would have.

If you read Article 30 of the GDPR regulations this will inform you that organisations with fewer than 250 employees will not be obligated by GDPR, however there will be several requirements that mean they probably still should comply.

All organisations must remember that even though the UK voted to leave the EU 'which has been successful' the GDPR must still apply to all UK organisations, if they are handling data with EU citizens, or has the potential to identify individuals within the EU.

Digital minister Matt Hancock has confirmed that the UK will replace the 1988 Data Protection Act (DPA) with legislation that mirrors the GDPR post-Brexit.

The legislation has been introduced to encourage organisations across the EU to take data protection more seriously. Please remember to stay aware that if you are to ignore the GDPR it comes with some fairly hefty fines/penalties, for those that do not comply with the new regulations. Organisations also need to bear in mind that if you are to use an individual's personal data in any way shape or form that they have not allowed you to do so, they can sue your organisation for compensation to recover for both material damage and non-material damage; For example something like distress.

If you have any uncertainty whether or not the GDPR applies to you, you must take into consideration how regularly handle personal data; this will includes present and past employees as well as supplies, not just customer's personal data. The ICO has also stated that any businesses affected by the DPA will also fall under the GDPR. But the key difference between the DPA and the GPDR is that the latter will be much stricter in what is defined as personal data.

ARE YOU READY FOR GDPR? WHITEPAPER

BRIGHTERDIRECTIONS.CO.UK

https://www.asa.org.uk/ - ASA statements/quotes

The GDPR will come into full effect by the 25th May 2018!

If you would like help with GDPR compliancy or any element of your marketing, please contact our expert team via the website www.brighterdirections.co.uk or call 01246 586330.