GDPR and My IT Support – A Guide

As the UK runs up to the implementation of GDPR on 25 May 2018 our clients are calling in asking us what are 'we' doing to ensure that they comply with GDPR. We are aware that nearly every company will be affected in some way by GDPR and many clients will be seeking guidance on what is required from an IT perspective. This guide is intended to provide a 4-step process for companies wishing to ensure they comply with the GDPR requirements.

Scope

Let us first define the scope of responsibilities.

What is expected of the client

It is the client's responsibility to examine their business and identify their "Data Assets". The data assets are essentially any information that could identify or be attributed to an individual person or group of people.
[GDPR data subjects are people; NOT businesses. GDPR does not apply to protecting business entities, only people.]

Once identified the client needs to ask four questions:

1) Why are they retaining this data and what is it used for?
2) What impact could the theft or distribution of this data have on the data subject?
3) What are the vulnerabilities of that data?
4) How can any potential risk be reduced or minimised?

What is expected of the IT supplier (Cutler IT)

We can assist you in assessing the vulnerabilities of your data assets and reducing these threats. This would be done in conjunction with you and within your budget constraints.
[Note – GDPR does NOT require that every threat is removed and data assets are totally secure. This would be unfeasible both practically and financially. However, the security around your data asset should reflect the threat assessment of its impact on the individual and its vulnerability.]

How to implement GDPR within your business

To implement the GDPR we would focus on following the guidelines which are built around IT and for our Office 365 clients, Microsoft have some recommended links. This can be found on the following Microsoft trust centre site. https://www.microsoft.com/en-us/TrustCenter (follow the link for GDPR)

Four steps to implementation

1) Discovery – What data do I have?
2) Manage – Why am I holding this/How am I processing it?
3) Protect – If I need it then how can I protect it?
4) Report – Manage requests for information and breach notifications

How to carry out the four steps

Step 1 – Discovery

In this step you need to revisit your business and 'discover' any personal or biometric data that relates to personal information. What exactly is personal or biometric data?

Personal – any data that relates to an identified or identifiable person (data subject); an identifiable person is one who can be identified directly or indirectly by reference to an identifier such as a name, number, location data, to one or more factors specific to the physical, genetic, mental, economic or social identity of that person[1]. In short, if you can link someone in any way with data – then it's personal.

Bio-metric data – personal data relating from specific technical processing relating to the physical, physiological or behavioural characteristics of a person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopy data[2]. i.e. photos, drawings and fingerprints.

The above data includes physical data such as papers, letters etc, however as this document relates to your IT systems we will restrict discussion to your IT infrastructure only.

Discovery will entail searching for files and data that relate to personal or biometric data on any device within your business. These may be on the following:

- Servers (shared file structures)
- Database applications, CRM systems and any applications you use in your business.
- Cloud based systems that hold personal data.
- PCs, desktops, laptops and tablets that are used for business.
- Shared drive devices such as NAS boxes etc.
- USB sticks, Backup tapes, CDs etc

For some this may be a big job but for most of our clients this will be quite simple as they do not hold personal client data. [**Please note that employee records, pay, and records are included and qualify as personal data**]

What am I looking for?

In simple terms anything that, if it fell into the wrong hands, then it could be damaging or embarrassing to an individual? This is files, documents, spreadsheet lists, photos, medical records, financial records.

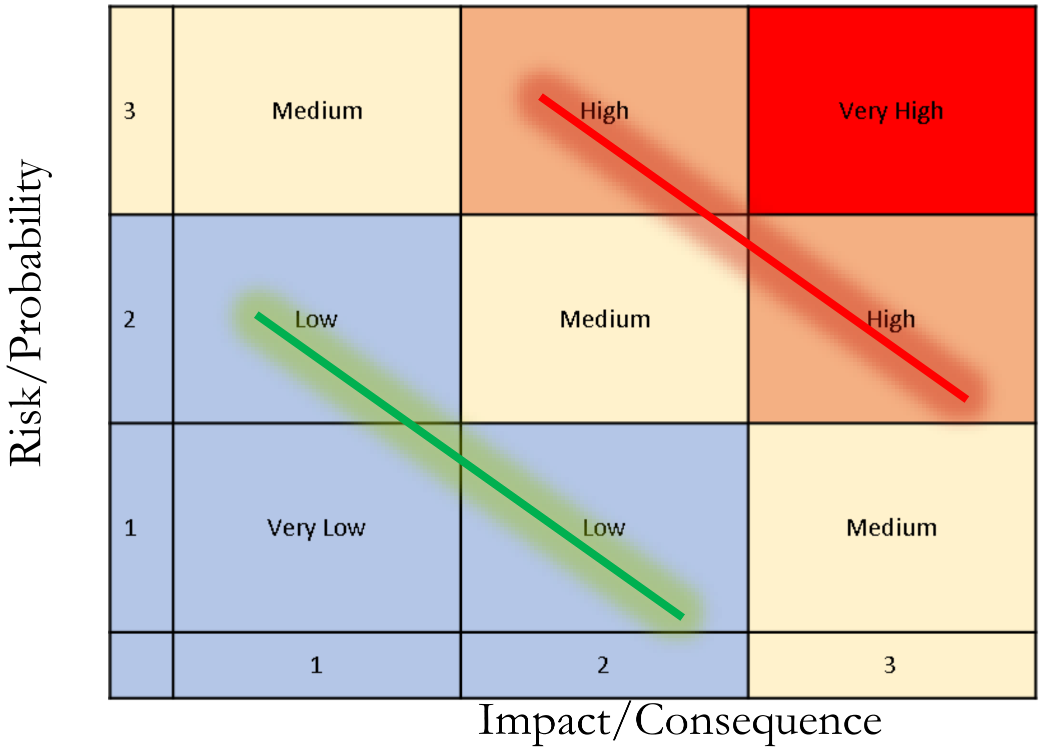
When you find the data you should then carry out a simple risk assessment on it.

[1] EU GDPR, Article 4(1) and GDPR a pocket guide by Ian Calder
[2] EU GDPR, Article 4(1) and GDPR a pocket guide by Ian Calder

How do I assess the risk this data carries

The diagram below illustrates a simple assessment chart for determining where your organisations data risk levels sit.

Consequence and Probability = Risk



3	Medium	High	Very High
2	Low	Medium	High
1	Very Low	Low	Medium
	1	2	3

When reviewing your data score the impact or consequence of it being disclosed between 1 and 3 (low and high), then score the risk or probability that this may happen. Once you have both scores the diagram will illustrate the data that you need to work on.

Step 2 -Manage the data

Now you have identified the data you need to ask some questions?

1) Why am I holding this data?
    a. Is this data relevant and necessary to running the business?
    b. If not – why am I keeping it. (what is my retention policy)
2) If I need it – how is it being processed and by whom?
3) Who has access to this data and why?
4) Has the person who this data belongs to, given permission to retain it.

[**The judgement of how these questions are answered is down to you as the client to decide. You may have a governing body or association that could advise you on the sensitivity of this data.**]

When you have decided what data you are retaining and processing, you need to decide who has access to the data and how you wish to control that access to protect your data.

Step 3 - Protect the Data Asset

We can assist you in setting up access security policies for your staff. We can also assist you in ring fencing secure data from non – secure data within your network/organisation.

In most cases simple security access policies will suffice and indeed they may well already be in place. Where data is identified as having a high impact then you may need to consider the following in conjunction with us:

- Where is the data held?
- Who has access to it?
- How easy is it for someone to get into this location?
- Are there any IT vulnerabilities that we are aware of?
- Do we need to run a penetration scan.
- Is this data removed from the building at all?

Together we can advise you on a course of action to ensure you maintain a security level you decide is appropriate for your organisation.

[**Remember GDPR does not insist that all risk is removed from the data asset – but it does require a reasonable and professional approach to your security policies**]

If you are a member of a professional body, association or adhere to laid down operating standards, it may be that the GDPR requirements are laid out in their latest documentation. We have found though that detail is poor in many cases as to what specific requirements should be implemented. In these cases please talk to us and we may be able to provide help to you in understanding your own requirements.

Cutler IT can assist you in all of the following IT checks.

- Desktop and server build and configuration, and network management security
- Firewall configuration security review
- Wireless network configuration
- Configuration of remote access solutions (including solutions for managed devices and BYOD)
- Build and configuration of laptops and other mobile devices, such as phones and tablets used for remote access
- Patching at operating system, application and firmware level
- File systems and database configuration security review

Step 4 – Manage Requests for Information and Reporting breaches

Although it is not primarily an IT subject you will need to ensure you have processes and housekeeping in your IT that allows for the following GDPR requirements.

Obtaining Consent

GDPR states that you cannot assume that a client is OK for you to use and process their data because they haven't complained. You now require a positive acceptance from them to continue to use it. However, if your business requires specific personal data to function, you may already have a consent form in place. It is worth taking independent advice in this area.

- The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese.

- The request for consent must be in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.

- Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to Access and The Right to be Forgotten

- Data subjects have right to obtain from the data controller, confirmation as to whether or not personal data concerning them is being processed.

- Known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in the regulations, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. You need to have a process for removing the data from your IT infrastructure.

Data Breaches

It is good business practice to have security policies for your business in place. This may cover what to do in the event of a breach and whether or not it requires to be reported. It is not always the case that breaches require reporting. If protection is in place to mitigate the data breach (e.g. the data stolen was encrypted) and no danger exists to the data subject there may be no need to contact them. If this is not the case then you have around 72 hrs to inform the governing body and the data subjects.

Organizations that process personal data need to:

- Keep records about the purposes and categories of processing
- The identity of third parties with whom data is shared; whether (and which) third countries receive personal data, and the legal basis of such transfers.
- Organisational and technical security measures.
- Data retention times that apply to various datasets.

Cutler IT – Access to client data

In order for Cutler IT to carry out its day to day business activities of supporting our clients' IT, we require to have administrative access to their systems. Our security and staff vetting policies are detailed in our terms and conditions and each staff member signs a non-disclosure form on joining the company. Where the client requires their own forms signed for non-disclosure this can be discussed and implemented.

It should be noted that there is currently no 'GDPR' security certification for third party companies that can be attained that will provide third party GDPR certificate you can use to certify your suppliers. It envisaged that this will be introduced as the UK splits away from EU directive and implements its own version of GDPR. Until then it is a European standard adopted into UK law.

In order to maintain auditability, only Cutler staff has access to the Admin password for Cutler but clients may have a separate admin account and password for their use.

It is our policy to request access from the client and no unattended access is carried out without first being authorised. Where an audit of the work carried out in a support session is required, we would use the 'Bomgar' system that records all detail of a support engineers work whilst logged into the clients machines.

We are happy to discuss any other measures you may require in order to confirm the trust relationship we have with you.

We hope that this document clarifies some issues for you and provides a framework for you to easily check your company for compliance to the new standard when it becomes law in May this year.

Author: D. J. Mitchell - CULTLER IT.

END OF DOCUMENT