JDI
Computer Services

JDI HOUSE, 5 CHURCH WALK, FULWOOD ROW, PRESTON, LANCASHIRE. PR2 6SZ

Making sure your company is GDPR compliant.

Big, medium sized or small, companies still need to make sure that they have taken suitable measures to protect the data they accumulate or process and handle it in line with these new rules on data protection. This encompasses many aspects from training staff on best practices to appointing a Data Protection Officer (DPO) and identifying where all their data rests.

APRIL 15, 2019

JDI COMPUTER SERVICES LIMITED
JDI House, 5 Church Walk, Preston, Lancashire. PR2 6SZ

This document is in Five sections: We look at why a "risk Assessment" is the best way of understanding your GDPR compliance exposure.

1.01 IT & Data governance - Audit all the information your organisation holds

You must set up a list of the personal data you hold and arrange it by type, i.e. names, addresses, phone numbers, and so on. You must also provide a source for each separate piece of information documented. *The JDI GDPR Risk Assessment handles this.*

1.02 IT & Data governance - Determine why you hold the information you do

GDPR requires you to establish a legal basis for collecting data, which you will need to outline in your privacy policy. Determining how and why you use data, for your own reference, will make it easier to communicate this to your customers. We go into consent further in this documentation, but it's not the most reliable basis for collecting data considering users can withdraw that consent at any time, so it's worth considering your options. *The JDI GDPR Risk Assessment handles this.*

1.03 IT & Data governance - Establish how you store data, and who it's shared with

This could be a list of internal databases but could also include offline stores and third-party storage providers. You must establish which parties you share your data with so that if you need to delete or amend that data, you can inform an associate organisation that they must also update their records. *The JDI GDPR Risk Assessment handles this.*

1.04 IT & Data governance - Document how data is processed

Organisations will need to outline all processing activities, including keeping the name and contact details of the data processors, as well as the categories of processing carried out - and the transfers of personal data to an 'adequate' third country (one that is outside the European Economic Area, but whose data protection measures are deemed adequate for data transfers) or international organisation. *The JDI GDPR Risk Assessment handles this.*

2.01 Customer awareness - Revamp your privacy policy

Organisations must write a clear and understandable privacy policy that is publicly accessible on their websites. This must clearly stipulate your lawful basis for data collection and processing in concise, easy to understand and clear language. Clear communication will help to build long-term customer trust in your organisation. *The JDI GDPR Risk Assessment handles this.*

2.02 Customer awareness - Refresh existing consents if necessary

Consent must be given freely, as well as being specific, informed and unambiguous; hinging on a positive opt-in. Under GDPR, you can't rely on pre-ticked boxes or opt-outs, nor bundle in consent with agreement to other terms and conditions. You must explain clearly and specifically why you're collecting certain data and what that data will be used for, plus which third-party controllers will be able to use that consent. You also need to make clear that users can withdraw their consent down the line and make it easy for them to do so.

You should also keep consents separate - if you're asking users to agree for you to do different things with their data, you'll need to ask for their consent to each of these things. Although you won't necessarily need to refresh all existing consents gathered pre-GDPR, if you rely on consent to process data, you will have to ensure existing user consents meet these higher GDPR standards or be ready to re-consent them.

2.03 Customer awareness - Highlight any third-party processors

Your customers and users need to be informed of the use of any third-party data processors or controllers, to which they should consent by accepting your privacy policy. Third-parties will need to respect your data subjects' rights just as strictly as your own organisation, and their involvement in processing data must be rigorously documented. *The JDI GDPR Risk Assessment handles this.*

3.01 Maintaining your customers' rights - Respect new and existing rights

You should examine your procedures to ensure they cover the new and existing rights customers have - including how you plan to delete personal data or provide data on request. *The JDI GDPR Risk Assessment handles this.*

3.02 Maintaining your customers' rights - Fulfilling Subject Access Requests (SARs)

People's requests to access the data you hold on them must be fulfilled within a month, instead of 40 days, and data must be provided in a structured, commonly-used format, and you cannot charge a fee. Consider implementing a system for users to easily access their own data online, to reduce the pressure on staff handling many SARs. More information from the ICO can be found (here). *The JDI GDPR Risk Assessment handles this.*

3.02 Maintaining your customers' rights - Right to rectification, restriction, and erasure

The new legislation outlines how users have more control over their personal data. The key to respecting these rights lies in understanding how your organisation plans to handle the flow of requests to amend any data inaccuracies, to comply with a demand that you stop processing someone's data, and to erase any personal data you hold on a subject or move it to another organisation at their request. *The JDI GDPR Risk Assessment handles this.*

4.01 Internal awareness and accountability - Staff training

A great many data breaches are inadvertent and involve a degree of human error by staff with access to internal systems. Training all your staff to be aware of how GDPR affects their daily work not only maximises your organisation's chances of full compliance but minimises any risk of suffering data loss or theft. More help from the ICO can be found (here). JDI offer bespoke onsite training in all aspects of GDPR for staff – Please contact us using the following Link

4.02 Internal awareness and accountability - Educate decision-makers

Setting up an accountability and governance framework, involving executives and senior members of staff in your organisation, is key to compliance. Involving senior staff is not only important in budgeting for the compliance process, but for identifying the areas that may be at risk, and ensuring each department has a specific readiness plan to execute. *The JDI GDPR Risk Assessment handles this.*

4.03 Internal awareness and accountability - Appoint a Data Protection Officer (DPO)

Your organisation must designate a DPO with the responsibility for data protection compliance if you carry out regular and systematic monitoring of individuals at scale, or large-scale processing of special categories of data, such as health records. The DPO must have the right knowledge, support and authority to carry out their duties effectively. The ICO has created a on-line tool to help you understand if you require a DPO of not (link). *The JDI GDPR Risk Assessment handles this. If you wish us to support, you in your DPO responsibilities then email us using this link*

4.04 Internal awareness and accountability - Carry out a Data Protection Impact Assessment (DPIA)

DPIAs are mandatory for certain organisations in cases where a new technology is being deployed, a profiling operation is likely to affect customers, or where there is processing of special categories of data on a large scale. DPIAs help to should establish how risky certain data processing activities are. Your organisation should consider where DPIAs are necessary, if at all, and how you run the process. The ICO has some useful advice about when and how to perform one. *The JDI GDPR Risk Assessment handles this.*

4.05 Internal awareness and accountability - Reporting data breaches

Any breaches involving **personal data** must be reported to the ICO within 72 hours - including what data has been lost, any consequences, and what countermeasures you've taken. Any loss in non-encrypted personal data must also be communicated to the data subjects involved. It's vital to cooperate with authorities as fully as possible to both minimise the scope for suffering penalties, and to ensure your reputation does not suffer any undue damage. *The JDI GDPR Risk Assessment handles this.*

5.01 Data Security - Data Protection

Data privacy has become a basic human right. With data breaches on the rise and the implementation of GDPR, then data protection needs to be the number one mandate for companies today. Too often companies must balance data protection risks with the pressure to move fast. GDPR tips the scales towards data privacy, meaning global businesses must rethink how they provide secure access to data throughout their organisation. *The JDI GDPR Risk Assessment handles this.*

5.01 Data Security - Managed Firewalls

GDPR mandates that businesses should secure their infrastructures using up-to-date technology which offers both situational awareness of potential threats and the ability to take 'preventative, corrective, and mitigating action," in almost real-time. This isn't simply a case of law-makers being overly-cautious. At a time when reports of high-profile ransomware attacks and businesses suffering huge financial losses after failing to keep data out of the wrong hands are all too common, technology which enables a business to quickly identify potential security breaches and take immediate action is vital for the long-term safety and success of any modern organisation.

How can technology achieve this in a way that neither triples your IT expenditure nor requires a complete overhaul of your entire infrastructure? You guessed it: ***A Managed Firewall***. A comprehensive solution that not only monitors and manages all incoming and outgoing network traffic but also provides greater protection against malware, ransomware and other security breaches than the standard firewalls typically provided by your ISP. *The JDI GDPR Risk Assessment handles this.*

5.02 Data Security - Humans and process errors

Although data breaches because of cyber-attacks get all the press, it is often negligence or a lack of basic processes, policies and procedures that result in data breaches.

The Information Commissioner's Office (ICO) compiles quarterly statistics about the main causes of reported data security incidents. In the last quarter, four of the five leading causes in cases where the ICO took action involved human errors and process failures:

Loss or theft of paperwork – 91 incidents
Data posted or faxed to incorrect recipient – 90 incidents
Data sent by email to incorrect recipient – 33 incidents
Insecure web page (including hacking) – 21 incidents
Loss or theft of unencrypted device – 28 incidents

4 of the 5 top causes of data breaches are because of human or process error