

DO YOU KNOW WHAT DATA YOUR COMPANY NEEDS TO DESTROY?

Posted on 03/05/2018



Category: [Uncategorized](#)



Many companies are unaware of how they are capturing data, how they are storing it, and how long they are permitted to keep it

All European markets have privacy legislation, but the European Union General Data Protection Regulation is a step forward. It harmonises the legislation in different countries and will protect the privacy and personal data of people when they are interacting with companies.

The amount of data in existence is multiplying so there needs to be some common rules regarding how it is handled. The fact is that people's personal data is becoming more exposed to risk – for example, the number of transactions involving the use of a credit card is increasing. It is now necessary for companies to know what data they have stored and where this data is stored. In reality, companies often do not know, so they need to find out what data they have. The current situation is that companies are often very conservative in their approach in that they keep all data, but under the GDPR, companies cannot keep everything, and they have to destroy some data. Companies need to understand that there are some individual rights that supersede the rights of companies.

With regard to regulation of data, the current situation is like having traffic laws but no police in the sense that all the inspections conducted by the Spanish data protection agency are reactive in nature. Consequently, companies do not really fear the consequences of not adequately protecting their customers' data. However, companies now face increasingly severe penalties if they disregard the data protection rights of consumers. For example, in some cases, the fines could be €20 million, or 4 per cent of the offending company's total worldwide annual turnover, whichever is higher. In addition to fines, firms also face the possibility of suffering severe damage to their reputation. This can be a disaster for a company, a reputation can take many years to build and then it can be lost with one single act. Meanwhile, if a company faces a large fine it can have an economic impact on all the company's staff – for example, it could mean that, this year, you do not get your bonus.

Effective data protection involves ensuring all levels of your organisation are aware of the procedures that need to be followed. All parties in your business need to be aware of the data protection plan. You need to know what the rights of your company are and what individuals' rights are. The company's chief executive officer must dictate the policy and the action to be taken, including training people and appointing a data protection officer (DPO).

The difficulty companies can face in this situation is that it can be difficult to find out what data you actually have. In addition, another challenge companies face is the change from keeping physical data records to digital records. You need to look at how the company is capturing data, and how it is storing it. You also need to determine exactly what is personal information and what is not. You also need to be aware of how long you are permitted to keep different types of information. For example, you have to keep accounting information for ten years, but there are some other types of information you can only keep for 24 hours.

Training is vital

You also need to provide training and carry out audits to ensure you have the right firewalls in place. With regard to appointing a DPO, it could be someone already on the payroll, you could recruit someone externally, or you could use a third party, such as a law firm. Regardless, you need to have somebody observing data protection processes.

Clients will want to see evidence of your data protection procedures. External partners will ask for information and certification, for example. You will have to comply with the GDPR if you want to work with major companies. Companies are in trouble if they are unaware of what GDPR is; you need to understand what information is affected and put in place processes.

At Iron Mountain we have considerable expertise in this field as we were involved in the GDPR from the very beginning. We help transform businesses into fully compliant operations by analysing what

information they have, what they are storing and where they store it. We split personal data from other data and ensure there are "destruction dates" for the relevant data. We also link digital and physical data.

Top companies have been fully aware of the GDPR for a long time, but for the 99 per cent of Spanish companies that are small and medium-sized, we can put together an easy questionnaire for them to answer in order to assess their needs.

Ignacio Chico is director general of Iron Mountain in Spain