PUTTING HR IN CONTROL OF GDPR

PUTTING HR IN CONTROL OF GDPR

The EU's General Data Protection Regulation is going to affect businesses of all sizes throughout the EU and beyond, and the one department that is going to be impacted irrespective of industry or any other business aspects is HR.

To HR leadership this is not going to come as any great surprise; HR departments are used to processing lots of personal data, including:

- Name
- Address and other geographic information
- Photographs
- Medical information (including doctors notes, reasons for sickness, details of employee disabilities)
- Employee performance records

But with GDPR coming into effect very soon, it's vital that HR ensures they are compliant and able to deal with it in the most efficient way possible. Here are some steps to take to make sure your HR department is ready to implement the new laws.

HR AND PAYROLL SYSTEMS

A key part of HR departments becoming and remaining compliant is having the right systems in place, that enable GDPR compliance in the way they process personal data. One of the largest uses of the data processed by HR is the payroll list, which many companies still send as a spreadsheet email attachment.

Using a single HR and Payroll system is an important step in helping firms not only become and maintain GDPR compliant, but also keeping the personal data that they collect and process safe, in a demonstrable way.

DATA CLASSIFICATION

Good HR and Payroll systems recognise the different types of data they process. This allows the data to be better categorised and segregated, which allows rules to be established, appropriate to the type of data being processed. Examples of this use of data classification include the ability to recognise that medical records are usually more sensitive than date of birth.

APPROPRIATE USER ACCESS MANAGEMENT

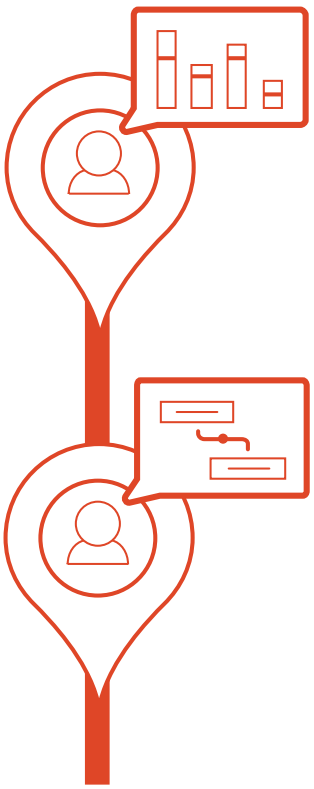
User access management is the way that most HR systems are able to ensure security of data, only allowing required levels of seniority access to certain data records. There are many systems on the market that do not do a good enough job of recognising this requirement; make sure that your HR system is not one of them.

DATA RETENTION AND DESTRUCTION

If you speak with many companies about how long they keep data, the answer is all too often, "We keep everything forever". Such an approach is not only ill-advised in these days of increasing cybersecurity threats and attacks, but it is also illegal under the GDPR, which requires that data only be retained for as long as is required by the purpose(s) that data subject gave consent for.

The ideal from an HR systems perspective is that as much of the processing and alerting around data retention is performed by the system as possible. This requires your HR system be able to be configured to support your data retention policy and identify any data that may have broken the retention policy - i.e which may fall outside retention guidelines.

Having identified the data that is approaching its data retention deadline, it is ideal that the HR system can cope with the requirement to retain the data for longer (a foreseeable requirement in certain cases) and identify the data for destruction when the retention date has expired.



VENDOR COMPLIANCE

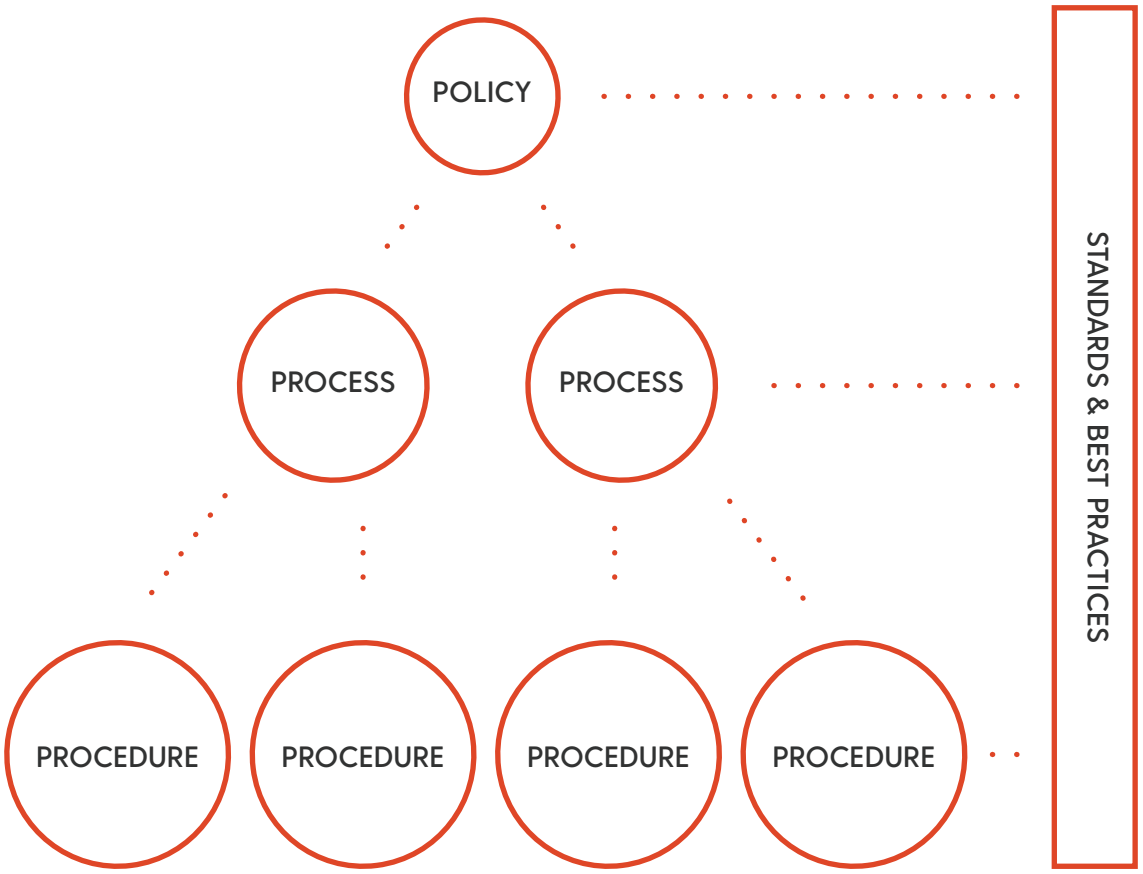
HR departments are not alone in their use of vendors. If, however, their organisation has not implemented a vendor management process, then HR will have to do so. Vendors to HR are very often data processors, processing personal data of varying degrees of sensitivity.

This means that it is vital that the organisation have a vendor management process in place to ensure that contracts are appropriate (including being compliant with the GDPR) and that they have the correct processes and procedures. These processes should also ensure that the vendor is adhering to SLAs and that those SLAs have sufficient time for the vendor to reply and allow the firm to maintain their own compliance.

POLICIES, PROCESSES AND PROCEDURES

The GDPR has an expectation that many policies will be in place, this including:

- Data security and privacy policy
- Data retention policy
- Business continuity policy



As the diagram above shows, for each policy, there will be at least one process (often several). Where ever possible these should, of course, be automated by your HR or other supporting systems; working in an HR department is hectic enough, without the creation of work that can be automated. Automated processes are favoured by regulators as they are far less likely to be circumvented or bypassed as part of a shortcut.

Ensure all of your processes and procedures are still appropriate. It is not unusual to find business processes that have become outdated or are no longer required. This kind of housekeeping can make your HR department more efficient and ensure compliance with the rules and regulations that are still appropriate and current.

WHAT IS A DATA BREACH?

The GDPR defines a data breach in Article 4 as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised. Disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This definition includes scenarios such as:

- Hacker activity
- Accidental loss of data
- Using data for a purpose other than those that consent was given
- Accidental (or deliberate) release of data to unauthorised staff or third parties

AGREE DATA BREACH PROCESS WITH YOUR CIO AND DPO

The GDPR requires that any data breach is dealt with, within 72 hours of its discovery.

This means that the organisation must take certain steps including:

- Triage the breach and ensure that it is not still ongoing
- Establish the extent of the breach (how many records of personal information have been taken, lost, misused, etc.)
- Establish the impact on the data subjects of this breach
- Notify the data protection authority (where appropriate)
- Notify data subjects (where appropriate)

The short timescale and the nature of the process to be undertaken means that no organisation can afford to not have a data breach plan in place ahead of its being needed.

If your organisation has a Data Protection Officer (a Data Protection Officer is a mandated role under the GDPR, particularly for organisations who process more than 5,000 records per year), then you should work with them and your organisation's CIO (or whoever is responsible for your organisation's IT) to ensure that the data breach plan is both in place and appropriate for the type of data and the risk appetite of the organisation as a whole, with a focus on the HR department in particular.

DIFFERENCES BETWEEN THE DPD AND THE GDPR

The Data Protection Directive (DPD) was enacted into UK law in 1998 as the Data Protection Act.

Whilst the GDPR builds upon the foundations laid by the DPD, there are several key differences that organisations need to be aware of:

Extraterritorial

GDPR is extraterritorial, this means that it doesn't matter where your organisation is based, you have to comply if you are processing EU residents' data.

Additional Data Subject Rights

There are a number of additional rights that have been conveyed on the Data Subject, including the right to data portability and the right to manual processing.

DPA Enforcement Powers

Data Protection Authorities have the right to ask organisations to demonstrate their compliance with the GDPR, they don't have to wait for a complaint to be made or a breach to occur, although these are still likely to the be the most common ways that organisations will encounter their DPA.

Fines

No explanation of some of the differences between the DPD and the GDPR would be complete without a mention of the increase in fines, these can be as high as the greater of €20m (£17m/~$21.75) or 4% of annual global revenue.

HAVE A PROJECT IN PLACE TO ENSURE DATA PRIVACY AND PROTECTION

Regulators such as the ICO in the UK have spoken about a soft landing for GDPR enforcement, but this is only for those who respect it. Companies who have ignored it or done nothing to prepare for it, will be those who will receive the greatest fines.

The quickest way to ensure that your organisation is on the right path and is able to demonstrate its commitment to GDPR is to undertake a GDPR assessment. If your firm already has a GDPR project underway, this will help guide any next steps and ensure that all areas required are covered to the appropriate depth. If your firm doesn't have a project in place yet and isn't sure where to start, a GDPR assessment will provide a roadmap to compliance that will serve as a high-level project plan and will demonstrate to a regulator that you are taking the GDPR seriously and have a compliance plan.

CONTACT US

Fifth Step provides services to executive and senior management to enhance their business' IT capabilities, governance and processes, as well as reducing risks from organisational change.

WHERE TO FIND FIFTH STEP

London

33 Queen Street, London,
EC4R 1BR

New York

1745 Broadway, New York,
NY 10019

Bermuda

Rosebank Building, 12
Bermudiana Road,
Hamilton HM 11


www.fifthstep.com


info@fifthstep.com


+44 (0)20 7193 1966


www.linkedin.com/company/fifth-step-ltd


@fifthstep

CONTACT XCD

Bristol

29 St. Augustines Parade
Bristol
BS1 4UL


www.peoplexcd.com


info@peoplexcd.com


+44 (0) 800 0432923


www.linkedin.com/company/xcd-limited/