simplisys
SERVICE DESK

GDPR – The responsibilities of the data controller?

Introduction

Responsibilities of Data Controllers

If your organisation runs a service management tool installed onsite or uses a SaaS based service management tool, such as a service desk or help desk application, then as we have seen in our last paper on the new GDPR requirements you are a **'Data Controller'**.

Being a data controller for the purposes of the GDPR comes with some key responsibilities that you will need to fulfil to ensure you, and your organisation stay within the law. These responsibilities all stem from the overriding principles contained within the regulations that require personal data to be collected and processed in a secure and transparent way ensuring the data's integrity.

The main responsibilities of data controllers with respect to processing data within a service desk environment include:

- To maintain records of all processing activities (Article 30 GDPR);
- To ensure a level of security (Article 32 GDPR);
- To notify the supervisory authorities in the event of a data breach (Article 33 GDPR);
- Specific obligations as regards transfer of data outside the EU (Chapter V GDPR);
- To assist data subjects with exercising their rights to privacy and data protection (Chapter III GDPR).

While all above obligations are important perhaps the key ones are the requirements relating to security, maintaining records and the rights of data subjects. We will be considering the rights of data subjects and the implications for your systems in the next paper. This paper considers security and record keeping.

Ensuring Security

Here we are discussing the security and integrity of personal data, which

inevitably involves securing internal IT systems and or ensuring the hosted service providers systems are secure. ISO27001 and Cyber Essentials accreditation are a good starting point here but it goes further…

Consideration needs to be given to the type of personal information being stored. Where there is a possibility of sensitive personal information being stored, such as the contents of documents uploaded to the system manually or included as attachments on emails it may be appropriate to encrypt these documents both in transit and at rest.

Another scenario for consideration is where the IT infrastructure hosting the service management system is used to host a number of different systems or applications. In this scenario there is a risk that a security weakness in one application could allow a hacker to access the service desk data from an unrelated application; can you be sure that both the data and processing is sufficiently segregated between diverse systems? The same sorts of questions arise around shared databases. You may need to consider ensuring the service desk application is running on dedicated infrastructure.

Also when somebody contacts your service desk team does the service management system allow you to confirm their identity before discussing a personal case? Perhaps via security questions or Employee reference number?

Maintaining Processing Records

The need to maintain records is often thought of as an ‘audit trail’ where a record of who did what is maintained. Data processing however requires more than that. The system will need to show not just who changed a given record but what they changed. Information regarding both the initial and final states is required as well as intermediate states.

This also applies to automated processes. Where an automated process has triggered an update for example the system should record the fact that the update was made by this autonomous process and the initial and final states of the record saved. It should be further noted that a key requirement of GDPR is the ability to demonstrate to Data Subjects that all data processing was fair.

But it isn’t just processing in terms of changing the records in the system that needs to be recorded. Another of the data subject’s rights require that the controller is able to tell him or her who has seen the data, so the system will need to additionally record who has opened the record even if no changes were made.

All records need to be easily accessible by standard 'reports' in the system, which can be produced in an ad-hoc manner to satisfy any requests for information by the data subject or the supervising national authority, in our case the Information Commissioner.

The need to maintain records extends beyond the actual processing of information. The underlying processes need to be documented in a way that is clear and transparent. For example workflow processes that allow automated processing to occur need to be presented in the system and potentially exportable in a simple to understand way. For example for workflows, it might be expected that the system represent the workflow as a graphical 'flow chart' rather than a list of instructions or for a business rule the system provides a simple and clear set of conditions and actions triggered by those conditions rather than a complex data base query.

Does your Service Desk Measure up?

Many Service Desk systems developed out of a requirement to manage fault tickets in an IT environment. It is therefore not surprising that neither record keeping nor the security of personal data was to the forefront of the developer's minds.

To move from these simple help desk / fault tracking systems into an enterprise wide service management solution means that GDPR and the responsibilities it places on data controllers and data processers needs to be an underlying guiding principle in the design and implementation of these systems.

It goes on... As mentioned above, the GDPR gives certain rights to Data Subjects and your service management solution needs to support you in delivering those rights.

We will look at data subject's rights and the impact on your responsibilities in our next paper.

References

The full text of the GDPR

Additional Resources