simplisys
SERVICE DESK

How will GDPR impact your Service Management Operations?

Introduction

Should you worry about GDPR?

Maybe, GDPR is a far reaching set of regulations; you might call it Data Protection Act on steroids.

To start with you need to understand the key terms:

Data Controller - The person(s) responsible for deciding what needs to be processed and why. (Article 4(7) GDPR)
Data Processor - The person(s) responsible for processing the data in accordance to the data controllers' instructions. (Article 4(8) GDPR)
Data Subjects - The individual(s) to whom the data being processed relates. (Article 4(1) GDPR)

In terms of a hosted Service desk the following are key players:

1. Data Controller is the organisation (Director Responsible) who is deciding what the Service needs to provide.
2. Data processor is the organisation providing the Service, it should be noted that there may be many Data processors including Employees who are responsible for running the system.
3. The Data Subjects are the uniquely identifiable individuals about whom the data is being processed.

Definition

GDPR (General Data Protection Regulations) are a set of regulations that give rights to data subjects, the people we support when using our service management tools, and set out the responsibilities of data controllers and data processors, the people controlling and operating the service desk.

This paper investigates if and how the GDPR regulations impact your service desk and the required functionality of the service desk to ensure you can comply with GDPR requirements.

The first thing to consider is, does GDPR even apply to your service desk? GDPR applies to any system, manual or automated procedure where personal data about individuals is processed. Individuals mean any living person whom you can uniquely identify from the data you hold or identified through combining your service desk records with other data

available to you or your organisation.

Who is an 'Identifiable Person'

So, what do we mean by uniquely identifying an individual?

An identifiable person is anybody who can be identified directly, or and this is important, indirectly. (Article 4(1) GDPR).

This identification can be via an identifier such as a name or identification number, employee number for example. However, if the individual can be identified by other means such as location or factors, either singly or in combination, such as physical, physiological, genetic, mental, economic, cultural or social identity then that person is considered identifiable.

Even recording a first name is enough if that can uniquely identify an individual knowing that he or she is an employee for example.

The identifying information doesn't even need to be held within the Service Management system, it is enough for a link or reference to be provided to another, possibly external, system e.g. linking back to your Active Directory system may be enough to uniquely identify an individual and thus bring the system into scope for GDPR.

Moreover the information used to identify an individual doesn't need to be stored in a structured format, in dedicated contact records for example. Simply receiving and processing an email to create a new ticket can be enough to qualify your system as being subject to GDPR.

What constitutes Personal Data?

The GDPR specifies a wide-ranging definition of what constitutes personal data. It is "any information relating to an identified or identifiable natural person ('data subject')" (Article 4(1) GDPR)

What should be noted here is the inclusiveness of the definition. You don't need to be storing / processing information of a sensitive nature to come under the GDPR, it is enough that you have ANY personal data about an individual.

It should be noted that even basic contact records recording an individual's name, work location and email address is enough. More importantly when you add tickets linked to that contact record, via your service desk, the amount of personal data relating to that individual grows exponentially and needs managing in terms of the regulations.

While it might be thought to be fairly simple to identify personal information i.e. data such as a person's email address, full name, date of birth and so on but sometimes the personal data we hold isn't so easily recognisable for example you might record a number of security questions within your service desk to enable you to validate who you are talking to when they call you for a password reset. Data such as mother's maiden name or name of the first school they went to, make this personal information in terms of the GDPR.

Beyond the basic information recorded about an individual certain classes of information are considered 'special' where additional rights and responsibilities are conferred by the regulations. (Article 9 GDPR)

Rights and responsibilities will be explored in the next paper.

Special types of information are defined as:

1. Data revealing racial or ethnic origin.
2. Data revealing political opinions.
3. Data revealing religious or philosophical beliefs.
4. Data revealing trade union membership.
5. Data concerning an individual health.
6. Data concerning a natural person's sex life or sexual orientation.
7. Biometric information, such as fingerprints, where this is used to identify a person.

Your system may not directly record such information in the contact record, but, can you be sure that such information isn't recorded in attachments added to tickets, in emails received by the system or even inferred based on information you hold?

For example, a ticket generated by an email received from an individual where a trade union representative has been copied could be used to infer trade union membership, or a change in working hours at specific times of the year may well be used to infer religious or even ethnic background.

What do we mean by 'Processing'?

Again, the GDPR definitions are wide ranging. Data processing can be defined as:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means including, but not limited to:

- Collection

- Recording
- Organisation
- Storage
- Adaptation or alteration
- Disclosure by transmission
- Dissemination or otherwise making available
- Combination
- Restriction
- Erasure or destruction

(Article 4(2) GDPR)

Effectively as soon as the information hits your Service management tool it is deemed to have been processed. Perform any activity based on that data and further processing has taken place. Note that the processing can be manual so even making a phone call based on information recorded, such as the contacts phone number and subsequently updating the ticket counts as processing.

Does your Service Desk Measure up?

It is almost certain that if you operate, or have others operate a service management system then that will fall within the scope of the GDPR controls.

In coming white papers we will be exploring what this means for you as a data controller or processor and to the individuals about whom you store information.

We will look at the core requirements of a good service management tool to enable you to not only comply with the GDPR requirements but to also evidence that compliance.

References

The full text of the GDPR

Additional Resources

Tel: 01275 240500
Fax: 01275 240501
sales@simplisys.co.uk