simplisys
SERVICE DESK

GDPR – Data Subjects Rights; Data Controllers Responsibilities

Introduction

The fourth paper in the series looking at the impact of the new GDPR (General Data Protection Regulations) coming in to force on 25th May 2018. This paper looks at the responsibilities of the Data Controllers delivering the data subjects rights; the next paper will explore how Data Processors should support Data Controllers running helpdesk/CRM software applications.

Data Controllers' responsibilities to Data Subjects

As well as direct responsibilities under the GDPR there are a number of responsibilities that a data controller has as a result of being accountable for ensuring the rights of data subjects are respected and maintained.

The rights in question, as we saw in the last paper, are:

- Right to access
- Right to rectification
- Right to erasure (Right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not to be subjected to automated individual decision-making

We will look at each of these in the context of the responsibilities it places on the data controller.

Right to Access (Article 15 GDPR.)

This right places on the data controller the responsibility for ensuring that any processing or storage of personal data is done in such a way that allows him / her to provide, on request by the data subject, details of any data held and who has access to it and when that access took or takes place.

Systems must be in place, or provided by your data processor or software, to identify, not only, if data is held about an individual but also the nature of the data, its disclosure actual and potential and whether or not it has been subject to automated decision making.

Right to Rectification (Article 16 GDPR) and Right to Erasure (Right to be forgotten) (Article 17)

These rights are about ensuring the data held about an individual is correct and only held if there is legal authority to do so. The key element here is that it applies to all information held about a data subject and not just active master records.

For example, if a data subject requires you to correct information help about him then that must be done in all copies of the data. This could not only include 'live' master records, say in a contact record, but also in any audit logs, secondary records such as records held in a different format or structure for reporting purposes and hot or warm standby facilities.

Requests to delete information may require your system to overwrite records with anonymising information rather than 'hard delete' to preserve data base integrity, in which case all copies must be identified, including those in long term archive or backups.

Right to Restriction of Processing (Article 18 GDPR) and Right to Object (Article 21 GDPR)

Both of these rights impose a requirement that personal data held about the individual not be subject to further processing.

In many cases simply deleting the records in question may fulfil the requirements but where this isn't possible, where a temporary halt to processing is needed to allow for corrections to be made or there are legal grounds for retaining the information then it must be possible to 'flag' the individuals records in some way as to prevent them from being processed.

Again, this restriction mechanism must be applied to any instances of the records in question. For example, a warm or hot standby system must also be configured with the processing restriction flag.

Right not to be Subjected to Automated Individual Decision-making (Article 22 GDPR)

Similar to the right to restrict or object to processing a data subject can request not to be subject to automated decision making. The requirement here is for the ability to restrict processing to be granular enough so as to allow normal processing, but restrict automated processing.

For example, where a system contains business rules that may authorise, or reject, a request for flexible working based on a rule set, for example the data subject's gender or ethnic background, then the system must allow the user to be excluded from such processing.

Conclusion

The requirement to enable data subjects to exercise their rights under GDPR requires some specific data access and processing functionality from any data processing systems you use rather than the rather more technical cyber security requirements imposed by the GDPRs direct requirements on Data Controllers.

Data controllers must ensure the systems they use are able to identify personal data, how and why it's processed and manage that processing at a granular, individual, level.

References

The full text of the GDPR

Additional Resources