The Data General
Apr 2019

BRIDGING THE COMMUNICATION GAP

IN THIS ISSUE

SAR Subject Access Request

Access requests is an interesting topic where organisations can easily get caught out. An SAR is a highly visible point of interaction between the organisation and the public. All that effort in Marketing and PR can go to waste if you get it wrong.

Templated responses are very important because you must ensure that you respond to requests in a coherent, compliant and consistent manner.

However, an SAR process is founded on knowing what data you are keeping, where it is, and how it flows inside and outside the organisation. Therefore, you must document what data you have and where it is located through a data map. You will also need a Record of Processing which is a mandatory document we will discuss in a later Newsletter.

Can I charge for Access Requests?

The short answer is no. Under the 1998 Act you could but not under the 2018 Act and this is because the 2018 Act changed many aspects of data management including who owns the data. Under the 2018 Act the individuals own the data even though you may be storing it. Hence data is now privately owned and individuals now have mandated Rights in law.

However excessive requests can be charged for. If you are going to charge someone you need to be very sure of your ground as the circumstances need to be exceptional, such as repeated requests for the same information. If someone is acting on behalf of a large number of people then this request would not be excessive and you cannot charge.

Many Privacy Policies on websites today still say that they will charge and that is a clear indicator that the business is unlikely to be compliant and will be investigated one day soon.

An SAR is based on Rights but what are they?

▷ Right to be Informed – Provision of 'fair processing information', typically through a Privacy Notice/Policy, to the Data Subject.

▷ Right of Access – Individuals have the right to access the Personal Data and supplementary information being held.

▷ Right to Rectification – Individuals can have their Personal Data rectified if it is inaccurate or incomplete.

▷ Right to Erasure – A withdrawal of consent to use of their Personal Data by either a client or employee may trigger the need to erase some, or all, of the Personal Data held.

▷ Right to Restriction of Processing – Individuals have a right to suppress processing of their Personal Data.

▷ Right of Data Portability – Individuals can obtain and reuse their Personal Data for their own purposes, and where feasible transferred to another provider.

▷ Right to object – Individuals have the right to object to use of their Personal Data for specific types of processing.

▷ Automated decision making/profiling – Individuals can object to automated decisions and insist on human intervention.

We are here to help and you can find us at PrimeConduct or Contact Us . We are happy to assist in evaluating suppliers for compliance.

FAST FACTS

14,000

14,000 data breaches have been logged with the Commissioner since 25th May 2018.

41,000

Complaints from the public have doubled from 21,000 to 41,000, suggesting increased public awareness.

30 Days

You have 30 days to respond to a Subject Access Request.

72 hours

To log a breach with the ICO and expect increased SAR at the same time.

FOR MORE INFORMATION

We are pragmatic, helpful and ethical.

We belong to the IAPP

PRIMECONDUCT
Contact us at PrimeConduct or Contact Us

SAR Management Process

Step 1 Verification

Before any action is taken on the Subject Access Request submitted, the identity of the Data Subject submitting it needs to be verified to establish the request is legitimate.

There are two ways to verify the Subject Access Request is Legitimate:

- The email address that the request comes from matches the email address held on record for the Data Subject.
- The postal address that the request come from matches the postal address held on record for the Data Subject.
- If the address information does not match then the Subject Access Request must not be processed and a notification of the request being submitted must be sent to the Data Subject.

Log and Document

The request needs to be logged with a Case number and stored appropriately. The log must also include date and time of receipt of the request.

Case Management Action

Each case and it's progress must be documented with appropriate review of actions taken. This should include a case close section which describes the outcome. Each action requires a time and date.

30 days to complete

The Subject Access Request should be completed, based on the process, within thirty days of the original submission date.

If there are legitimate reasons why the request cannot be completed within the thirty days timescale, the Data Subject must be notified of this – together with the cause, a target timescale for completion, and the means of escalating this to the Information Commissioners Office (ICO) if they are not satisfied.

Escalate to ICO?

If you have notified the individual of an extended period to resolve the request then you also be prepared to answer questions from the ICO.

Risk Register Update

Any impact of the request and/or completion or incompletion should be considered as an item for the Risk Register.

Resolution Report

In any professionally managed process there needs to be a close to the incident particularly if resolving the request involved technical changes, process changes or re-training. This report documents the outcomes and decisions taken.