A practical guide to system requirements for GDPR in salesforce crm

Introduction

The General Data Protection Regulation is enacted by the European Union as of 25 May 2018. The purpose is to give EU individuals more power and control over their personal information. As a consequence, organizations must be able to justify why they are processing any individual's data. This is not intended as an exhaustive list of items but it overs the headline requirements.

Individual Object

The new Individual object in salesforce crm is a good start but it needs to be added to in order to fulfil the requirements of the GDPR. For example, there is no way to store the lawful basis as to why an individual's data is being processed.

Lawful Basis

One of pre-defined 6 lawful basis must be assigned (of which Consent is only one) against every name along with information that corroborates the lawful basis. In addition, there will be a date range applicable; in the case of Consent, the UK's Information Commissioner's Office (http://www.ico.org.uk/) has said that consent decays with time, so records need an expiry date by which time it will need to be reconsented – or deleted; in the case of Legitimate Interest, the additional information field needs to say why it was decided that Legitimate Interest was assigned.

Processing Reasons

The assigned Lawful Basis applies to a specific processing reason. Processing reasons will be whatever your organization uses the data for. For example, sales & marketing, newsletters, executing a contract, analysis, customer service. In addition, the processing reason will be applicable to a particular product (or product group) or service. Examples would be "pet insurance marketing", "car insurance marketing" etc.

Channels

For each category individuals can decide what channels they would prefer to be used. For example, phone, email, SMS, post.

Privacy Details Search

In practice sales and marketing people need to be able to quickly identify which records in their database are available for any particular campaign. For example, you may need to select all the records that have an active lawful basis "next week" for a certain category for a phone campaign; or you may want to select all those with Consent not active next week (ie expiring), then they can be reconsented before it expires; or you may need to select all those records that do not have an active lawful basis and decide whether the records should be deleted.

Deleted records

If an individual requests that you delete their data (and it is warranted), it is good to be able to show when it was deleted – either because they ask for confirmation or you may need to double check.

Data management

The fact that the new regulation stipulates that the lawful basis could be time dependant, and that data is constantly changing, means that someone needs to be constantly monitoring the state of data in the database. Various things will be happening all the time, for example:

- Consents expiring (soon)
    - Once a consent has expired you can no longer contact the individual, so you need to contact them before the consent expires in order to get it extended
- Consents expired
    - Once a consent has expired most likely the data will need to be deleted (immediately)
- Individuals becoming customers
    - As a customer a new processing reason needs to be applied to the individual with the lawful basis of "Performance of a contract". This facilitates communication with regards the customer contract
- Individuals ceasing to be customers
    - Assuming there is a lawful basis of "Performance of a contract" applied to the individual, this will need to be removed.
- Individuals updating channel preferences
    - Ensuring individual is only contacted using their preferred channels
- Individuals giving consent
    - Updating the lawful basis, record how consent was gained, and set the expiry date
- Individuals withdrawing consent
    - Updating the consent record. Remember that there may still be another lawful basis that can be use (eg Legitimate Interest)
- Individuals requesting to the deleted
    - If the delete request is valid (eg if they are a customer you wouldn't delete it) then the data must be deleted within 30 days
- Subject Access Request
    - The simplest way is to have a merge document with all the relevant fields to give the customer the information you have stored about them
- Individuals with another lawful basis becoming active or inactive
    - Remember that there are 6 lawful basis's that can be used:
        - Consent
        - Legitimate Interest
        - Performance of a contract
        - Protecting a vital interest
        - Compliance with a legal obligation
        - Public interest

With all this going on, someone needs to make sure the database is always up to date. A suite of reports and dashboards to keep on top of it all would be invaluable!

For more information on the DataPro Tools app that manages data within GDPR visit: www.dataprotools.co.uk