Serving EU Data Subject Rights

Creating Value With GDPR: Practical Steps

20th February 2017

Dr. Phil Thomas
GDPR Executive Architect IBM Analytics
philip_thomas@uk.ibm.com

Matt Wetton
GDPR Growth Lead for Financial Services
mattwetton@uk.ibm.com

Jon Asprey
Financial Services Sector Leader – Industry Solutions
jon.asprey@uk.ibm.com
Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

References to GDPR are references to REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Data subjects rights in relation to the GDPR

- Rectification & Erasure
- Subject Access Rights
- Objection & Intervention
- Notice & Transparency
- Consent Management
- Data Protection Impact Assessment
- Safeguards / Access Control
- Data Transfer
- Data Portability
- Breach Notification
- Subject Access Rights
- Notice & Transparency
- Consent Management
- Data Protection Impact Assessment
- Safeguards / Access Control
- Data Transfer
- Data Portability
- Breach Notification
A data subject centric approach

A data subject is offered an experience in a channel, enabled by a set of capabilities.
Challenges to overcome when it comes to the right of access

- Rectification & Erasure
- Objection & Intervention
- Data Portability
- Consent
- Breach
- Complaint / Dispute

- uncertainty of demand volume;
- identity of the requestor;
- time limits to respond;
- nature of personal data;
- increased risk from data flow,
- trigger to other rights
Tracing the realisation of the right of access from a set of capabilities

**Subject Access Rights**

- Regulations & Requirements Management
- Communications Management
- Case Management
- Data Discovery
- Data Subject Identification
- Rights Execution
- Master Data Management
- Data Masking
- Access Control
- Security Monitoring

**GDPR Capability Framework**

- Governance
- People & Communications
- Processes
- Data
- Security
- Compliance Demonstration
- Data Protection Impact Assessment
- Data Transfer
- Safeguards/Access Control
- Consent Management
- Data Protection Breach Notification
- Data Portability & Erasure
- Notice & Transparency
- Objection & Intervention
- Subject Access Rights
- Subject Identification
- Rights Execution
The ICO provides a code of practice for subject access

Subject access code of practice

What information is an individual entitled to?

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the personal data; and
- given details of the source of the data (where this is available).

An individual can also request information about the reasoning behind any automated decisions taken about him or her, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret).

Subject access provides a right for the requester to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply copies of original documents, but you are not obliged to do this.

3 important differences are the reduction in time to respond, the extended definition of personal data and the removal of ability to charge
Recital 59: Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

Recital 63: Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data.
What does the GDPR say about SARs: Article 15

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
What does the GDPR say about SARs: Article 12

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
Capability Focus: Case Management

- Access to content and data
- Action through workflows and dynamic tasks
- Assignment of tasks according to role
- Analytics on case progression
- Automation of tasks where feasible

- Limited, discretionary deviation from predefined process flow
- Monitoring of case progression and triggering of escalation where necessary
- End to end case recorded for audit purposes (accountability of compliance)

**DELIVERING THE RIGHT CONTENT:**
Business content related to the case is assembled.

**AT THE RIGHT TIME:**
Workflows are launched, in the forms of tasks, based on the decisions made by the workers.

**A case is opened**

**TO MAKE THE RIGHT DECISIONS:**
Workers use the content and their expertise to drive the case.

**A case is closed**
Simplified access to data and reduced labour for managing these data by establishing a single source of truth underpinned by flexible integration patterns and notification capabilities.

Complete identification of data by Golden Record* including linkage to unstructured data in documents and individual customer records in other systems based on probabilistic matching.
Outcomes we’re trying to demonstrate

- **Data Subject perspective:**
  - Ability to make access request and review results simply and straightforwardly, through their preferred channel

- **Data Controller perspective:**
  - Clear, defined, repeatable process
  - Fully auditable outcomes
  - Ability to efficiently deal with SAR’s (automated vs manual)
  - Monitoring of processes individually to ensure on track for timely completion, and escalate / keep data subject informed where required
  - Monitoring of overall statistics (e.g. time to complete, team utilisation) to highlight and better inform resourcing and process design decisions
Welcome to IBM Case Manager - Privacy Management Solution

User name:
p8admin

Password:

Log In
### Phased Implementation Approach

<table>
<thead>
<tr>
<th>Crawl</th>
<th>Walk</th>
<th>Jog</th>
<th>Run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff trained</td>
<td>Processes defined in orchestration tool</td>
<td>Full automation enabled</td>
<td>Engagement with data subjects through web and mobile channels</td>
</tr>
<tr>
<td>Processes defined and documented</td>
<td>Some steps automated</td>
<td>Automated search and retrieval of personal info via APIs</td>
<td>Correlation of cases to achieve a complete view of data subject right requests</td>
</tr>
<tr>
<td>Processing steps performed manually</td>
<td>Handoff of subprocesses where required</td>
<td>Proactive monitoring, alerting and escalation of process instances</td>
<td>Established reporting capability summarising evidence for Regulator</td>
</tr>
<tr>
<td>Monitoring and reporting enabled</td>
<td></td>
<td>Predictive reporting</td>
<td></td>
</tr>
</tbody>
</table>

© 2017 IBM UK & Ireland