A Mapping of GDPR to Common Features

Matt Clapham
Director of Cybersecurity for Software and Cloud
GE Healthcare
@ProdSec
By the time I’m done today, you’ll know a key set of features a product should have for GDPR readiness.
Agenda

- Disclaimer
- How we got to now in GDPR
- GDPR Rights for Feature Guidance
- Creation and Review of Features
- List of Features by GDPR right
- Application and Practical Example
- Q&A
I Am Not Anyone’s Lawyer

- Everyone deserves good privacy
- Want to meet or exceed...
  - User expectations
  - Regulations
  - Customer needs
- Works for us as a starting point
- Double-check my work in your context
The Path to GDPR Analysis

KEEP CALM and COMPLY WITH GDPR

This Photo by Unknown Author is licensed under CC BY-SA-NC
The Nine GDPR “Rights”

- Right to Information
- Right of Access
- Right of Rectification
- Right to be Forgotten
- Right to Restrict Processing
- Right to Data Portability
- Right of Notification
- Right to Object
- Right to Bring Class Actions
Individuals have a right to know what type of data is being collected about them and how it will be used.
Right of Access

Individuals have a right to access the personal data held about them, regardless of format or storage location.

This Photo by Unknown Author is licensed under CC BY-NC
Right of Rectification

Individuals have a right to get the information about them corrected if there are any errors.
Right to be Forgotten

Individuals have a right to request data about them be removed/erased from storage when there is no longer a valid reason to hold it.
Right to Restrict Processing

Individuals have a right to exclude their information from shared processing solutions.
Right to Data Portability

Individuals have a right to request and receive an export (in a common format) of all data held about them by the system.
Right of Notification

Individuals have a right to be notified of any disclosure, change, or correction of their information.
Right to Object

Individuals have a right to challenge and/or question automated decisions made about them or on their behalf.
Right to Bring Class Actions

Individuals have a right request group action on their behalf against an organization holding their data.
Feature Brainstorming, Development, and Review

This Photo by Unknown Author is licensed under CC BY-SA-NC
Features Listed and Grouped by GDPR Right

- **Right to Information**
  - Have a posted or configurable privacy policy
  - Have contacts for questions/updates
  - End user license agreement confirmation

- **Right of Access**
  - Have a way for users to see “what do you know about me?”

- **Right of Rectification**
  - Have a way for users to change/update what the system knows about them

- **Right to be Forgotten**
  - Delete as much as possible (except as legally required)
  - Hidden from searches where cannot be deleted (see legal)
  - Remove individual’s information from logs (see legal)
  - What does “forgotten” mean to your product?
  - Remove or phase-out individual’s information from backups (see legal)
  - Audit trail of request and result

- **Right to Restrict Processing**
  - Acquire user consent for data usage
  - Follow user’s consent decision (as much as possible)
  - Under age tracking with parent approval
  - Allow/halt to correct a decision based on automated processing
  - Opt out of demographic class

- **Right to Data Portability**
  - Have a way for users to download “what you know about me”
  - Have a way for users to export entire set of records
  - Have a way to choose format of data export

- **Right of Notification**
  - Have a way to notify users if/when privacy policy changes
  - See who accessed my stuff and when
  - Have a way to notify users if/when a privacy incident occurs

- **Right to object**
  - Notify on cookies use by site
  - Have an unsubscribe for spam
  - Opt-in to marketing messaging and ids by default
  - Have a way for user to change consent choice for marketing
  - Have a way to re-check consent on change of EULA or privacy policy
  - Have a way to track consent for various use types based on metadata tagging

- **Right to Bring Class Actions**
  - Notify on cookies use by site
<table>
<thead>
<tr>
<th>Right to Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Have a posted or configurable privacy policy</strong></td>
</tr>
<tr>
<td>• Provide a link to a posted legally reviewed privacy policy for users to read</td>
</tr>
<tr>
<td><strong>Have contacts for questions/updates</strong></td>
</tr>
<tr>
<td>• Provide a list of contact points (phone numbers, e-mail addresses, etc.) for Privacy questions or concerns (may be posted within privacy policy)</td>
</tr>
<tr>
<td><strong>End user license agreement confirmation</strong></td>
</tr>
<tr>
<td>• Request the user to confirm the license agreement (including reference to the associated privacy policy) at account creation or first launch</td>
</tr>
</tbody>
</table>
Right of Access

Have a way for users to see "what do you know about me?"

• Provide a feature for users, customers, or other authorized representatives to see all appropriate detail known about the end user.
Right of Rectification

Have a way for users to change/update what the system knows about them

• Provide a feature to allow users to self-service appropriate information updates
Right to be Forgotten

What does "forgotten" mean to your product?

- Define the constraints for a "Right to be Forgotten" request including potential legal requirements to retain data

Audit trail of request and result

- Provide an audit feature of who did what privacy actions when

Remove or phase-out individual's information from backups (see legal)

- Provide feature or mechanism to remove user’s information from backup data (over time a period of time, if appropriate)
### Right to be Forgotten, Continued

<table>
<thead>
<tr>
<th>Feature/Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete as much as possible (except as legally required)</strong></td>
<td>• Provide a feature and/or process to remove data as much as possible within applicable retention laws</td>
</tr>
<tr>
<td><strong>Hidden from searches where cannot be deleted (see legal)</strong></td>
<td>• Provide a mechanism to hide users from search results where information cannot legally be deleted</td>
</tr>
<tr>
<td><strong>Remove individual’s information from logs (see legal)</strong></td>
<td>• Excise individual’s data (PI/PII/PHI) from logs as defined and constrained by law. (i.e. keep PHI out of logs)</td>
</tr>
</tbody>
</table>
Right to Restrict Processing

Remove or phase-out of backups
• Remove expired/deleted individual’s data from backup history as appropriate

Acquire user consent for data usage
• Provide a feature to confirm the individual granted permission to use their data for specific purpose

Follow user's consent decision (as much as possible)
• Data tagged with consent information regarding acceptable uses
Right to Restrict Processing, Continued

- **Underage tracking with parent approval**: Provide a feature to associate underage users with a privacy decision maker (e.g. parent or guardian).

- **Allow humans to correct a decision based on automated processing**: Provide a way for authorized humans to correct errant data processing decision results.

- **Opt in/out of demographic data**: Provide a way for users to opt in/out of having their information used in demographic calculations.
Right to Restrict Processing, Continued Again

- Opt in/out of pseudonymization
  - Provide a way for users to opt in/out of having their information used in pseudonymized data sets

- Have a way for users to control who can view detail about them
  - Provide a way for users to specify which service providers are allowed to view their record (where appropriate for direct data access)

- Age gate cross-over
  - Provide a feature to verify consent when a user comes of age
## Right to Data Portability

<table>
<thead>
<tr>
<th>Have a way for users to download &quot;what you know about me&quot;</th>
<th>• Provide a method for users to download their entire record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have a way for users to export entire set of records</td>
<td>• Provide a feature or mechanism for a user to move all data from one service provider to another</td>
</tr>
<tr>
<td>Have a way to choose format of data export</td>
<td>• Provide a format picking mechanism when users export data</td>
</tr>
</tbody>
</table>
Right of Notification

- Have a feature to inform users of EULA or privacy policy changes
- Provide an automated way to audit who looked at what records
- Have a feature to automatically notify of users impacted by any privacy incident (e.g. breach)
<table>
<thead>
<tr>
<th>Right to Object</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify on cookies use by site</td>
<td>• Notify the user if cookies will be placed in browser cache</td>
</tr>
<tr>
<td>Have an unsubscribe for spam</td>
<td>• Allow the user to undo a previous opt-in for marketing messages</td>
</tr>
<tr>
<td>Opt-in to marketing messaging</td>
<td>• Require opt-in (by default) user consent to be included in or</td>
</tr>
<tr>
<td>and data by default</td>
<td>receive marketing messages</td>
</tr>
</tbody>
</table>
Right to Object, Continued

Have a way for user to change consent choice for demographics/marketing

- Allow the user to undo a previous opt-in for data usage by demographics or marketing systems

Have a way to re-check consent on change of EULA or privacy policy

- Provide a feature to re-confirm a user's consent upon notification data usage changes

Have a way to track consent for various use types based on metadata tagging

- Provide a method describe users consent to various data usage scenarios as it flows throughout the system
Right to Bring Class Actions

This space (un)intentionally left blank.
Known Gaps

- Feature collections is unevenly distributed
- Retention policies aren’t really discussed
- Better feature specificity needed
- Privacy law changes need review/incorporation
- Data processors underrepresented
- No way to answer the controller vs. processor question
- More self-service features
Apply What You Have Learned Today

● Next week you should:
  – Identify a target project that is GDPR impacted
  – Consult with your GDPR legal counsel

● In the first three months you should:
  – Add all these features to the project backlog
  – Evaluate each in context and create user stories as appropriate

● Within six months you should:
  – Implement at least one feature from each right (category)
## A Sample Implementation for Products

<table>
<thead>
<tr>
<th>Feature</th>
<th>Brief Description</th>
<th>Privacy Counsel Ratings</th>
<th>Individual Product Team Assessment and/or User Story</th>
<th>GDPR: Right to Information</th>
<th>GDPR: Right of Access</th>
<th>GDPR: Right of Rectification</th>
<th>GDPR: Right to be forgotten</th>
<th>GDPR: Right to restrict processing</th>
<th>GDPR: Right to data portability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove or phase-out of backups</td>
<td>Remove expired/deleted patient data from backup history as appropriate</td>
<td>Required</td>
<td>Both</td>
<td>High</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Acquire user consent for data usage</td>
<td>Provide a feature to confirm the patient granted permission to use his/her data for specific purpose.</td>
<td>Maybe Required</td>
<td>Controller</td>
<td>High</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have a way for users to control who can view detail about them</td>
<td>Provide a way patients can specify which medical providers are allowed to view medical record (where appropriate for direct patient access)</td>
<td>Not required</td>
<td>Controller</td>
<td>Low</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age gate cross-over</td>
<td>Provide a feature to verify consent when a user/patient comes of age</td>
<td>Required</td>
<td>Controller</td>
<td>Low</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow user’s consent decision (as much as possible)</td>
<td>Data tagged with consent information regarding acceptable uses</td>
<td>Required</td>
<td>Both</td>
<td>Medium</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under age tracking with parent approval</td>
<td>Provide a feature to associate underage patients with a privacy decision maker (e.g. parent or guardian)</td>
<td>Required</td>
<td>Controller</td>
<td>Medium</td>
<td>TRUE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recap

- GDPR analysis
- GDPR “rights”
- Feature development
- Feature review
- Features list
- Practical application
Thank you!

Matt Clapham, CISSP