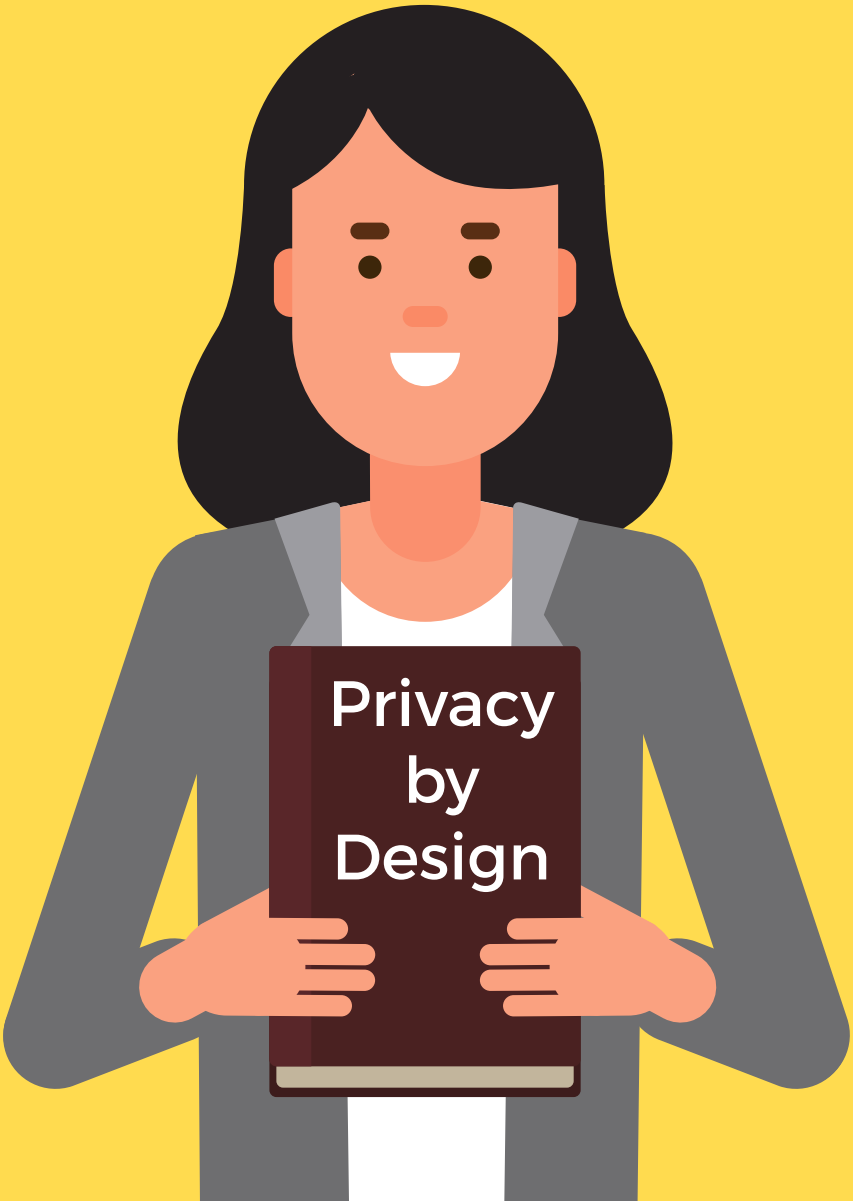
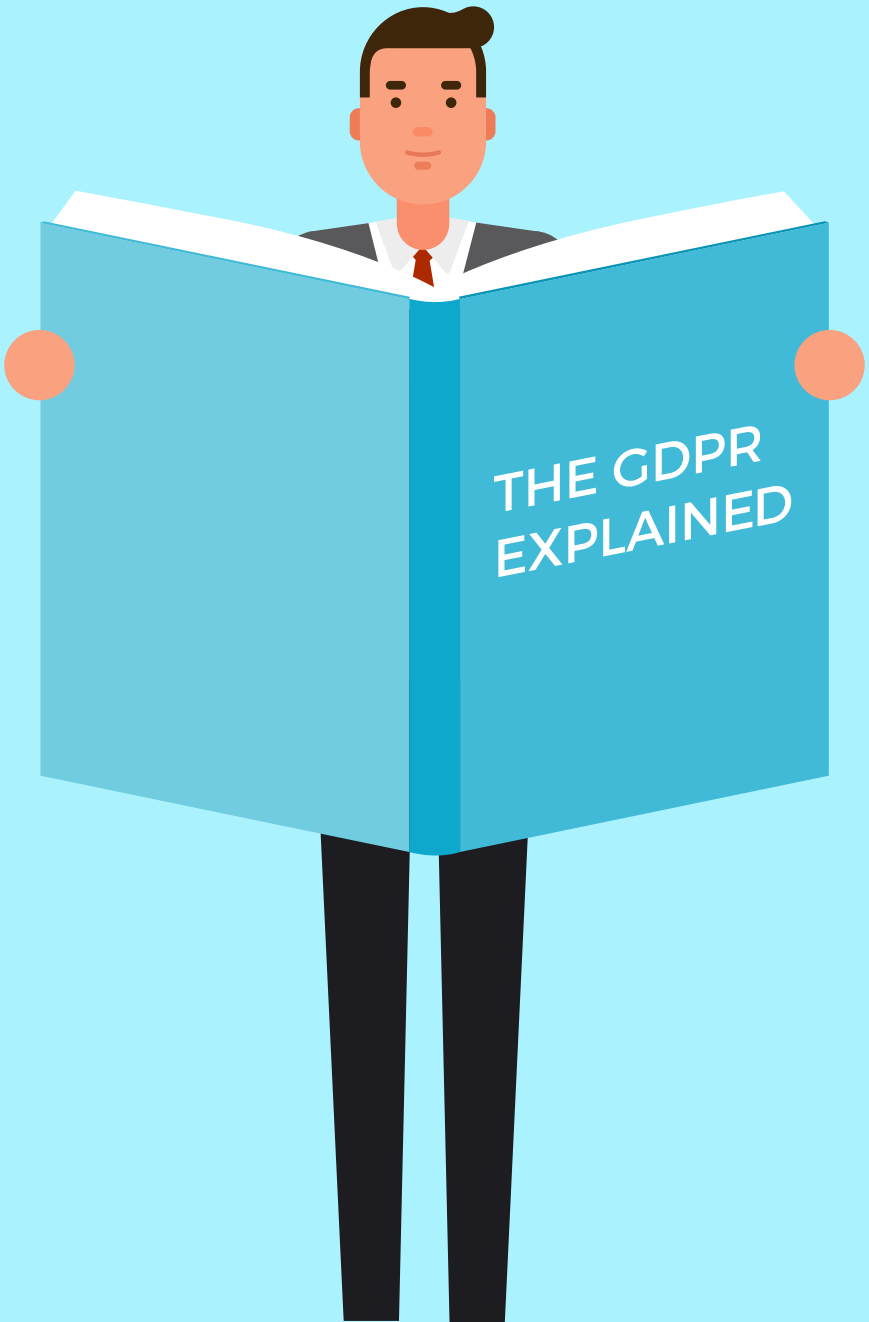
Tips for privacy by design - GDPR



CONSIDER:
How is this project impacting data privacy? How can we develop products/new functionality to lessen the impact and exposure of data privacy?

IN PRACTICE:
To remain transparent & accountable under GDPR, product development notes and descriptions need to highlight how we, the company addresses these considerations within our the development process.



1: CONSIDER: Are we minimizing data being collected?

IN PRACTICE: Wherever & to the fullest extent possible, develop our products such that a limited amount of information is required to fulfil the processing tasks.

2: CONSIDER: Are we collecting any data we don't need, if so, can we avoid this?

IN PRACTICE: Make sure the limited data fields needed are documented for each product and that the implementation teams know what fields are *required* to complete the processing.

IN PRACTICE: Goal is limit customer data in our system to data required for the processing tasks.

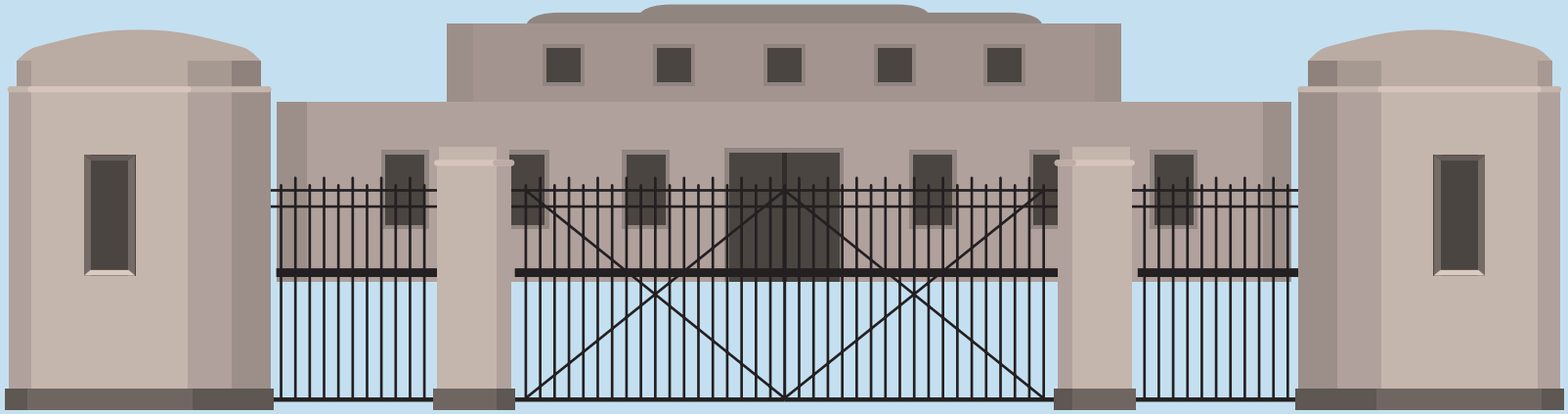
3: CONSIDER: Are we anonymizing, pseudonymizing, & encrypting the data where possible?

IN PRACTICE: If data is "**anonymized**" under **GDPR**, it is **IMPOSSIBLE** to relate the data back to an identifiable individual (and in some countries it is **criminal** to be able to do so)

IN PRACTICE: If data is "**pseudonymized**" under **GDPR**, it is tied together with a **unique ID** # (or other non-personal identifier) instead of a **name**, **email**, **IP address**, etc.

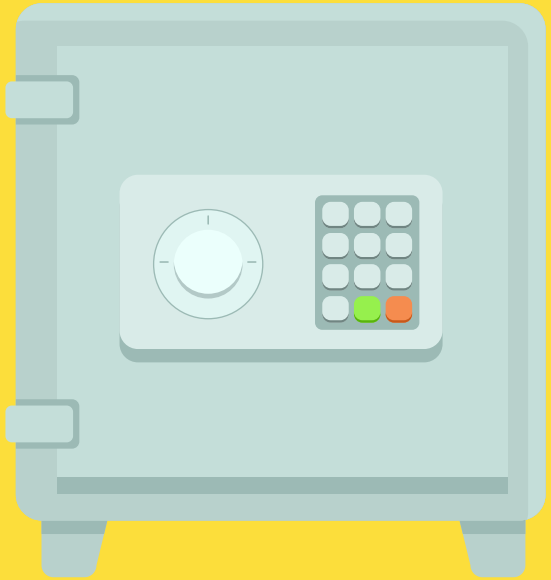
IN PRACTICE: Make efforts to incorporate **anonymization** and **pseudonymization** to your product development plans and **roadmaps**. Note, **anonymization** is preferred where possible.

IN PRACTICE: If we are unable to anonymize or **pseudonymize** the data, we need to make efforts to **incorporate more data encryption** as a less-protective (but better than nothing) measure.



4: CONSIDER: Are we conducting all processing in-house/storing data in the same locations as currently permitted?

IN PRACTICE: When data is routing to a **new location/data center**, the **Data Protection Committee** must be **notified** of the **new transfer location**.



5: CONSIDER: Have you completed the required vendor questionnaire and submitted to legal?

IN PRACTICE: Before a new product/ new functionality will be released for **general availability** to sales the **product manager** should **complete** a **questionnaire describing** the new **product features** and submit it for processing.

Required as part of that **submission**: a **data map** for new product/ functionality & completed record of processing spreadsheet

All issues and matters relating arising from the above topics should be reviewed with the company's privacy team, and all high risk activities need to undergo a privacy impact assessment – now required under GDPR.