GDPR Compliance Requirement

Article 6: Lawfulness of processing

- Explicitly capture and associate one or more permissions with an individual record as per Article 7 defining conditions of consent.
- Alternately to associate a record of lawful processing because of a legal or contractual obligation or a justification.

Article 9: Processing of special categories of personal data.

- Mark any identified special category personal data and to restrict access and use of such data.
- Associate a record of lawful processing based on one of the 10 exceptions listed in Article 9

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject

- For any requests that data subjects have regarding personal data, the CRM should provide capabilities to provide the information in an easily understandable format.
- The CRM should document the fact that this request has been made as well as executed.

Article 16: Right to rectification

- If a data subject requests that inaccurate information contained be corrected and if that information is contained in the CRM system, then the controller needs to correct this data and provide a record that this process has occurred.
- Capabilities to notify the data subject that the inaccurate information has been corrected in the CRM.

Article 17: Right to erasure

- If a data subject requires data to be erased, then the CRM must be able to do the following:
  - If valid, erase the data and send a confirmation to the data subject and attach a data entry to the data subject's record that this has occurred
  - If invalid, then send a notification to the data subject and attach a data entry to the EU resident's record that this has not occurred.

Article 18: Right to restriction

- If a data subject invokes Article 16 or 17 where the CRM is involved and the request requires time for investigation before a decision can be made, then the CRM should provide capabilities that temporarily removes that information from use by authorised individuals.
- The data subject should be notified and a record of that notification should be captured.

Article 19: Notification obligation

- If any rectification or erasure of personal data or restriction of processing was carried out in accordance with the above articles, then the controller must notify each recipient to whom the personal data have been disclosed of the exact rectification, erasure or restriction. The CRM system should provide the capability to notify these recipients.

- The controller shall also inform the data subject about those recipients if the data subject requests it. The fact that the EU resident has requested this should be acknowledged and tracked by the CRM.

Article 20: Right to portability

- A data subject has the right to have their personal data transferred to another provider. While the CRM system may not be the primary source of this information (telephone numbers, health records, bank transfer details, etc.), it might be used to consolidate this data. If this is the case, then the CRM system should provide the capability to provide the required information in a form that can be transferred to an alternate provider.
- The data subject should be notified and a record of that notification should be captured.

Article 21: Right to object

- If the CRM uses any form of automated decision making (such as next best product, next best offer, risk assessment, potential for purchase, etc. for any type of profiling purposes) that uses personal data and the data subject objects to that information being used, then the CRM system should have the capability to eliminate that personal data being used for the automated decision making.
- The fact that the data subject has requested this should be acknowledged and tracked by the CRM.

Article 25: Ability to limit access to personal data.

Provide the capability to:

- Identify and mark exactly what personal data is contained within the CRM.
- Set up specific access groups of individuals and other IT systems on a need to process/need to know basis.
- Ensure only the minimum amount of personal data is actually surfaced to each group of individuals or other IT systems to complete required tasks.
- Generate reports showing which personal data was accessible to which groups.

Article 34: Notification of a data breach

- When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller shall communicate the personal data breach to the data subject without undue delay.
- The fact that a breach has happened should be acknowledged and tracked by the CRM.