

# General Data Protection Regulation (GDPR)

## Dapresy Statement

### Background

The General Data Protection Regulation (GDPR) is an update to the privacy rights for individuals that unites the current privacy legislation across the EU and updates it to provide a single set of rules which relate to the processing of personal data in the context of new technology and globalization. The legislation comes into force on the 25 May 2018.

Any organization that is involved in the processing of personal data of EU citizens is obliged to comply with the regulations. Personal data has a broad definition and includes name, date of birth, education, general defining characteristics through to cookies, photographs, videos, IP addresses, and so forth. There are special categories of personal data which primarily relate to genetic and biometric data, which covers information such as sexual orientation, politics and race, which have more stringent requirements for processing.

### Controller and Processor Relationship

Dapresy acts as a data processor to its customers, who act as the data controller. Under the GDPR the data controllers are obliged to use data processors that implement correct measures for compliance with the new regulations.

Data controllers have responsibility for defining purposes and means of processing personal data to ensure compliance with the GDPR. Dapresy recommend that customers seek independent legal advice regarding their commitments under the GDPR to ensure that they are not in breach of the new regulations.

### Legal Requirements

Article 6 of the EU publication which laid out the GDPR regulations [(EU) 2016/679] defines the 6 core requirements for lawful data processing:

- A - Consent - the appropriate permissions have been acquired
- B - Contractual - the data is required for the fulfilment of a contract to which the subject has agreed to or is subject to
- C - Legal obligation - to comply with the law
- D - Vital interest - to protect the individual or another person
- E - Public interest - for an official function with a clear basis in law
- F - Legitimate interests - to provide a service for the subject such as quality assurance

Further requirements for special category data are defined in article 9. If your survey data is using special category data it is important to review these rules as well.

## Dapresy GDPR compliance

### Overall Plan

A full audit of all systems to identify where personal information is stored has been carried out. This has identified what the purpose of that information is and ensured the minimization of the storage of sensitive data.

### Technical Commitment

Dapresy's infrastructure and software are implemented using best practice security measures with regular audits.

A general principle of avoiding redundant data is implemented.

When receiving data, local storage of files is not allowed, and online storage is used with at rest encryption without the possibility for local synchronization.

Expiry dates on mails identified as containing personal identifiers is set, such as survey data with sensitive information, providing for automatic deletion.

If sensitive information is required to be sent via electronic mail it is encrypted.

All private identifying information will be stored as short a time as possible.

Our backup policy is deliberately defined to be a short time period.

Incident notifications are communicated to clients promptly and with full transparency.

A process to respond to customer requests for removal of personally identifying information in a timely manner is in place.

### Personnel Commitment

All Dapresy employees are required to complete a specific GDPR training and awareness course, all employees must also sign a confidentiality agreement.

### Data Controller Requirements

Ensure privacy notices and consent forms are present wherever data is collected.

Establish procedures to respond to the individuals' requests for access, update, restriction and erasure.

Document the basis on which the data is being processed, under which of the criteria outlined in article 6 as described above

Limit the use of data to the purpose for which it was collected.

Implement appropriate security measures and ensure use of secure protocols to prevent access breaches

### How Dapresy Can Help You

Dapresy Pro has good support for recoding data and for data deletion when required.

We have added functions for the support of GDPR to include filters based on Open ended variables such as email addresses etc. which makes it easier to clean and recode data for specific persons which is highly relevant with the anonymization regulations.

The ability to recode data permanently and remove personal information from the data which is a requirement for the data minimization policies.

Dapresy Pro had functionality to recode data automatically after a certain period which makes it easier to meet data retention requirements.

Support for permanently deleting respondents to meet the GDPR right to be forgotten rules.