Data protection policy
Flex Applications data deletion policy

Responsible: Flex Applications, DPM
Approved by: Flex Applications, MD

1. The Flex Applications data deletion policy

The Flex Applications data deletion policy describes when different kinds of data in Flex Applications shall be deleted. When processing personal data, Flex Applications always has one of the following two roles and the data deletion rules apply per role:

1.1 Flex Applications is a Data Controller ("Flex Applications owned data")

Being a Data Controller, Flex Applications decides the purpose of the data processing, what tools / systems we use to process the data and we also decide how long we need to keep the data.

Examples where Flex Applications is the Data Controller for the personal data:
- Flex Applications employees
- Persons applying for a job in Flex Applications
- Customer contact persons in support tickets
- Customer contact persons, leads and prospects we do marketing activities or similar towards (in CRM systems)
- Vendor/partner contact persons (in contract systems etc.)
- Log files used to keep the systems up & running, to detect errors and to handle incidents
- NPS/customer satisfaction tools like Wootric
- Any processors used as part of the above

> **Flex Applications data deletion policy**:
> Personal data shall be deleted whenever it is no longer necessary to process the personal data to fulfil the purpose it was collected for, at the latest **3 years after last registered activity**. Exceptions might be possible if there is a legitimate purpose for processing the data longer than 3 years, in such cases please contact the Group legal team.

For **personal data about Flex Applications employees other rules** apply.

1.2 Flex Applications is a Data Processor ("customer owned data")

Being a Data Processor, Flex Applications acts upon instructions from the Data Controller (our customer). The instructions are given through Data Processing Agreements and contracts/terms with our customers and written instructions from the customers.

Examples where Flex Applications is the Data Processor for the personal data:
- Products we develop and sell to customers
- Products we are a reseller of, depending on the contract
- Backups and any copies of production data to other environments
- Internal systems used to the support of the products, if more than just the contact person details
- Any sub processors used for the above

Flex Applications is responsible for the data processing as long as we process/keep the data. Note our role might change to being a Data Controller - with all its obligations - if we do not delete the data as required when the customer terminates the agreement with us.

Deletion of customer's data should not depend on the customer requesting deletion, this should happen as part of the termination of the agreement.

Flex Applications data deletion policy:
The GDPR states that data shall be deleted **without any delay** when the customer has terminated their contract with Flex Applications.

- Customer backups for user support are deleted when the ticket is closed.
- Customer database backups at our hosting provider, are deleted 30 days after the database has been deleted in the production environment.
- Customer data is deleted in agreement with the customer or at the latest one month after the termination of contract. The customer is always given the opportunity to export the data or receive the data in another way agreed with the customer. All this is stated in the contract.

2. How to comply with this policy

1. Ensure you have a **data deletion policy** for your product, it is not enough to refer to this policy.

   The local data deletion policy for each products should be a **high level** document (no requirements to the format), describing
   - What triggers data deletion
   - Responsibilities
   - Retention times / how long you keep the different types of data incl backup (high level)
   - Link to more detailed descriptions in other documents if relevant
   - Owner of document and last updated date (Confluence/Google tracking ok)

2. Ensure you have deleted all data according to your data deletion policy so you are **compliant as of now.**

3. Ensure deletion is done according to your data deletion policy **going forward**.

4. Ensure relevant persons are **informed** of your data deletion policy.

3. If using Flex Applications Connect IdP as your identity provider

It is important to always make API-calls to Flex Applications Connect IdP whenever customer data (represented as user accounts and tenants) shall be deleted.

Each integrated product is responsible for removing their data from Flex Applications Connect IdP. If you have deleted customer data already, but not done the deletions in Flex Applications Connect IdP, please do that immediately.

4. Customers with multiple contracts with Flex Applications

The customer might have more than one contract with Flex Applications. This guideline gives directions only regarding the current service where the customer terminated the contract.

If there is customer data shared/used by other products/services in Flex Applications, then deletion of such data must be a coordinated effort, so the customer can still use the remaining services without disruption.

5. Other legislation

Flex Applications is obliged to comply with the GDPR. Other legislation, such as **bookkeeping / accounting / archive / case specific legislation** applies in most cases to the customer, not Flex Applications.

If a customer leaves Flex Applications, we need to delete the data after giving the customer the possibility to get an export of the data. It is up to the customer to find alternative storing methods or enter into an agreement with Flex Applications for archive / look up access to the data.

6. Export of data

We are obliged to be able to give the customer **an export** of their data so they can comply with other legislation. If this is not possible, a solution might be to give the customer a look-up licence for some defined time. In such cases, a customer contract and a data processing agreement must be signed, since we still process the data.

To give away **look-up licences** for free makes it harder to comply with the GDPR, as the customer will not be frequently reminded that we still keep the data.

7. Questions?

In case of questions contact the Data Protection Manager in your company or Visma Group Legal, data protection team.