Visma Business product line GDPR documentation

Chapter 1

General Data Protection Regulation (GDPR)

Topics:

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy. The enforcement date is the 25th of May 2018 for all EU countries. Norway being not part of the EU will have to convert the EU regulations into national law.

Who does the GDPR affect?

The GDPR not only applies to organisations located within the EU but it will also apply to organisations located outside of the EU if they offer goods or services to, or monitor the behaviour of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

How does Visma prepare for GDPR

Visma naturally sets out to ensure that all of our software services, to the very best of our efforts, are compliant with the GDPR. Therefore, we have designed a comprehensive framework specifically with the GDPR in mind, comprised of the following main components:

- Training for our employees
- Privacy and data protection built into development and production
- Dedicated data protection manager
- A revised data processing agreement

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

Visma as a provider for cloud and on premises software focuses heavily on this area to ensure our customers will be able to comply with the new regulations. This document will provide guidelines for the Visma Business product line in order to set up the system in a way to support the new requirements according to GDPR. However, Visma Business is a very flexible and highly customisable ERP system. Each company may use the system differently and may store different types of data in the various Visma solutions.

It is also important to understand that software/tools do not have to comply with GDPR; it is always a company who needs to ensure that all processes, including the way how they use their software/tools comply with the principle of GDPR.

Following this document alone cannot be used as an acceptance criteria for GDPR compliance. It is very common that other systems (non Visma systems) are in use and store either personal or sensitive data. Each company needs to verify their own practices when using the Visma

Business product line or other systems and verify that they have a process in place which is in line with the new regulations.

This document will focus on what needs to be considered when running the Visma Business product line with the following products:

- Visma Business
- Visma Business Regnskapsbyrå
- Visma User Directory
- Visma Reporting
- Visma Document Center
- Visma ERP POS
- Visma Zpider*

Visma Business or Visma Document Center are often connected with Visma.net cloud services like Visma.net AutoInvoice, Visma AutoPay or Visma.net Approval. Over the upcoming years we will see even more functionality moving from the on premises software to cloud solutions. This document covers the guidelines for connecting to these services in a secure way. More information about security and privacy can be found here:

- *https://www.visma.com/privacy/*
- *https://www.visma.com/trust-centre/*

* Visma Zpider is a product in pure maintenance mode and will not be covered by the new terms of service.

General aspects

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Data subject rights which affect functionality in our software

The following list summarizes the most relevant rights for a data subject in the context of the Visma Business product line

Right to Access:

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects

Right to be Forgotten:

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability:

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a "commonly use and machine readable format" and have the right to transmit that data to another controller.

Privacy by Design:

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - "The controller shall implement appropriate technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects". Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Use of data in the Visma Business product line

The Visma Business product line applications come with a set of tables and fields which can be used to store and process data. If fields are not used as intended (main purpose of the field) in the applications then functionality provided by Visma might not be enough to comply with GDPR requirements. This does not only apply to the standard fields provided by all applications, it also applies to free text fields or new fields added to the database by the data model extension tool. The tools provided by Visma for GDPR compliance rely on a standard use of the system. According to the standard use of the Visma Business product line there is no sensitive data stored in the system (with the exception of payroll systems like Visma Lønn and accounting transactions in the ERP created by payroll systems). If a company engages in large scale processing of sensitive personal data (outside the payroll process) then it needs to appoint a Data Protection Officer (DPO). The DPO must be involved when decisions are made regarding what sensitive personal data should be stored in Visma delivered systems and how access control should be handled for that type of data.

Visma Business

Use of data in Visma Business.

In Visma Business personal data can be found in the following tables:

- **Associate** table (customers, suppliers, contacts, employees)
- **Order** table (customer info)
- **Order document**/**Order document line** table
- **Customer document** table,

- **User** table

Sensitive personal data can be found by combining information from the following tables (if a payroll application is in use)

- **Account no.** in **General ledger transaction** table specifying the trade union membership account
- Combined with the **Empl. no.** referring to an employee in the **Associate** table

Any custom-made deviation requires also adjustments to the tools (for example layouts) provided by Visma. This is the responsibility of the data owner.

Visma Document Center

Use of data in Visma Document Center.

Visma Document Center stores a minimum of personal data including user's name and e-mail address plus supplier contact names and e-mail addresses. Login credentials are stored either in Visma User Directory or the ERP and not in Visma Document Center.

Visma User Directory

Use of data in Visma User Directory.

Visma User Directory stores personal data in form of user information.

Visma ERP POS

Use of data in Visma ERP POS.

Visma ERP POS stores personal data in form of user information and it synchronizes customers and employees with the ERP database.

Visma Reporting

Use of data in Visma Reporting.

Visma Reporting does not store personal or sensitive data.

Visma Zpider

Use of data in Visma Zpider.

Visma Zpider stores personal data in form of user information and customer information.

Where is data stored

The Visma Business product line delivery stores data in many different locations.

This chapter covers the locations of data stored for all product line applications.

Storage of backups

It is recommended to back up data produced by Visma applications on a regular basis. This kind of service is usually offered by companies who are hosting Visma Business product line products for their customers or it needs to be implemented by each company hosting the software on their own servers. Backups should include the databases and also files locally stored. These backups are also subject to GDPR regulations.

Use of backups

Using backups in test environments or making them available for 3rd parties (like Visma partners, or Visma support) will expose the information in the data to additional people. Special procedures need to be followed to ensure the content of the data is treated in line with GDPR. The Data Protection Officer should be involved when creating these procedures.

Visma Business

Visma Business stores data in the following locations.

Databases

- Visma Business system database (default naming: vbsys)
  - User information
- Visma Business company databases (default naming: F0001, F000x)
  - Customers, suppliers, contact persons, users, employees, orders, order and customer documents with personal information

- The databases can be extended with the use of Data Model Extension tool; it allows to create entirely new tables but also to add additional fields into existing tables; any type of information can be stored in these fields
- The existing database also contains a large amount of so called "free" fields which are meant to be used individually by all customers depending on their needs; any type of information can be stored in these fields
- Attachments can contain any content and it is not possible to verify it by Visma Business; attachments are used in the following cases
  - **Order attachment** table (attachments added by the company running Visma Business; full control what is attached)
  - **Document** table (attachments coming in from external sources; no control over the content)
  - **Incoming accounting document** table (attachments coming in from external sources; no control over the content)
  - **Incoming document** table (attachments coming in from external sources; no control over the content)

Locally stored files

- Log files are stored in `ProgramData` folder on the server and client machines.
- In the **System information** table in Visma Business it is possible to do several file path settings; these will determine where certain files will be stored locally
  - PDF documents
  - Memo files
  - Etc

Cookies used for embedded pages

- Visma.net pages
- Visma Reporting Web Client

Visma Document Center

Visma Document Center stores data in the following locations.

Databases

- Visma Document Center database
  - Visma Document Center system database (default naming: VDC_SYSTEMDB)
  - Visma Document Center company tables (stored in each of the ERP's company databases; default naming: VW_table_name)
  - Visma Document Center company views (stored in each of the ERP's company databases; default naming: VW_view_name)
  - Attachment handling (attachments can contain any content and it is not possible to verify it by Visma Document Center); attachments are used with incoming documents such as supplier invoices, credit notes and other documents.

Locally stored files

- Log files are stored in `ProgramData` folder on the server and client machines
- Visma Document Center is also storing files locally:
  - Server
    - Document data files (default location `c:\ProgramData\Visma\Visma Document Center\` or can be set by the ERP)
    - XML default stylesheets (in `c:\ProgramData\Visma\Visma.Workflow.Server\XmlStylesheet\`)
    - Log files are stored based on version (in `c:\ProgramData\Visma\Visma.Workflow.Server\`)
    - License files (DocumentCenterLicense.lic and/or DocumentCenterDemoLicense.lic in `c:\ProgramData\Visma\Visma.Workflow.Server\`)
    - Email settings (EmailSchedule.xml and SentTimes.xml in `c:\ProgramData\Visma\Visma.Workflow.Server\`)
    - Server variables file for the user running the server (in `c:\Users\user.name\AppData\Local\Visma\Visma Document Center\`)
  - Client
    - Log files are stored based on version

- User specific files: DataGridSettings, Filters; VismaUserDirectory export logs (usually in `c:\Users\user.name\AppData\Local\Visma\Visma Document Center\`)

Visma User Directory

Visma User Directory stores data in the following locations.

Databases

- Visma User Directory database
  - User information

Locally stored files

- Log files are stored in `ProgramData` folder on the server and client machines.

Visma ERP POS

Visma ERP POS stores data in the following locations.

Databases

- Visma ERP POS database
  - User information
  - Customer information

Locally stored files

- Log files are stored in `ProgramData` folder on the server and client machines.

Visma Reporting

Visma Reporting stores data in the following locations.

Databases

Visma Reporting does not use its own database. All data is taken from the connected applications like the ERP

Locally stored files

- Log files are stored in `ProgramData` folder on the server and client machines.

Visma Zpider

Visma Zpider stores data in the following locations.

Databases

- Visma Zpider database
  - User information
  - Customer information
  - Order information

Locally stored files

- Log files are stored in `\Program Files (x86)\Visma\Zpider` folder on the server (if the default path has been used during installation.

Data exchange across applications

In order to provide seamless integrations between Visma products data needs to be exchanged.

The products mentioned in the introduction part (Visma Business product line products locally installed) share or exchange data between each other in a secure way. However, in typical installations more than locally installed products are in use. There are two types of applications in general:

- Visma owned cloud services like Visma AutoPay, Visma.net AutoReport, Visma.net AutoInvoice, Visma Storage, etc... connected to the locally installed products
- 3rd party applications (off-the-shelf products) or custom-made applications
  - using the API of the locally installed Visma Business product line applications
  - going directly to the databases of the different applications and reading data or updating data/creating new records

Visma is fully committed to providing state-of-the-art data security, to all hybrid combinations of on-premise systems and networked solutions our clients operate. By using the Visma On Premises Gateway add-on service, you can setup a secure communication channel between your Visma on-premise system and your networked Visma solution. The data flow between the client's on-premise installation and any network resource will be protected by industry standard SSH encryption. Installation of the Visma On Premises Gateway is simple and requires no special technical knowledge or resources. For further questions or more in-depth information, please get in touch with us at *trust@visma.com*.

This document does not cover the GDPR integrity anymore as soon as data is exchanged between the on premises installed Visma Business product line and 3rd party applications. You need to contact the 3rd party vendors and verify that their products are secure and in line with GDPR regulations. This also applies to custom made integrations which add or retrieve data from Visma Business product line products.

Data can also be transferred via export from Visma Business or Visma Document Center. Both applications provide functionality which allows to store all data or a subset of it to file. Data stored like that is also subject to GDPR.

Sharing of data

What needs to be considered when data is shared with third parties.

Support is often provided by third parties (from the perspective of a data owner). Visma partners or Visma itself is one of these third parties. Besides descriptions on how to reproduce a case it is sometimes necessary to provide configuration files or even a copy of the actual database. This is also subject to GDPR because information is shared with third parties. Each company needs to have procedures in place to cover these scenarios. Depending on the nature (personal/sensitive) of the shared data different actions need to be taken between the data owner and the third party providing support (for example Visma or Visma partners) before exposing information to them. It is up to each company to define their own process in order to comply with GDPR when exposing data to third parties.

Request for removing personal/sensitive data

An individual may request to remove personal data (from the Visma system if it contains such information). These requests need to be verified against existing accounting laws in the various countries (accounting regulations usually require the storage of accounting document and invoice document for many years). Accounting laws override the GDPR.

If the individual is entitled to have his/her personal data removed from the Visma system because the data/documents are not covered by accounting regulations anymore then the data owner needs to follow this request.

Visma Business provides a set of layouts which will enable the search for entities with personal information (if the data owner has used the system according to the intended purpose; if free text fields or new fields are used for storing personal data then these layouts have to be adapted by the data owner manually).

Contacts, customers, suppliers (in special cases), employee records, user records, order documents and customer documents contain personal data. Memos can also contain personal or even sensitive information. That needs to be verified when a request for removing of data is in process. In order to keep the database integrity, it will not be possible to delete all entities (for example if accounting transactions are connected to a customer). In cases where a deletion is not possible the data must be anonymized by the data owner (by updating all fields where personal data is stored). From version 13.00.0 of Visma Business it is possible to delete order documents and customer documents. Customers or suppliers requesting to delete their data needs to be handled with care because these entities can have transactions associated with them; the following steps need to be considered:

- Are there transactions which need to be kept according to national bookkeeping rules? If this is the case then we cannot remove or anonymize data because the customer/supplier information is still subject to regulations overriding the right to be forgotten according to GDPR
- If there are no transactions at all on the customer/supplier then the records can be deleted
- If there are only old transactions (not covered by the bookkeeping regulations) then the following should be done:
  - Delete completed orders for the customer/supplier
  - Delete order documents (this is possible starting from version 13.00.0)
  - Delete customer documents (this is possible starting from version 13.00.0)
  - Delete attachments
  - Create a new customer/supplier which will be used to store old transactions
  - Enter the number of the newly created customer into the **New customer no.** field in the **Associate** table for the customer who requested data deletion
  - Enter the number of the newly created supplier into the **New supplier no.** field in the **Associate** table for the suppliers who requested data deletion

- Run the **Change Customer no./Supplier no.** processing in the **Associate** table; this will change all accounting records and product transactions to the new customer/supplier number; all references to the old customer/supplier number will be gone
- Delete the customer/supplier from the **Associate** table

If documents have been sent via the Microsoft Office Outlook integration then these documents will be archived in the **sent** folder in your email client. These documents are also part of GDPR regulations.

Secure setup of the Visma Business product line

How to setup and configure our applications in order to provide maximum security to your data.

GDPR is more than personal or sensitive data. As a company dealing with that kind of data it is important to have full control over your business systems. That includes security of your data (firewalls, password policies, etc…) a waterproof process for granting access rights (with internal approval routines and documentation), a good overview on who has access to what and good education of the employees handling GDPR relevant data.

This section will focus on how to set up the Visma Business product line in the best way to comply with security aspects, the right amount of logging (audit trail) and keeping an overview over people who have access to the systems.

Secure infrastructure

The Visma Business product line relies first and foremost on a secure setup of the Windows environment. If the different products are installed on different machines within the Windows environment then the communication between these machines needs to be protected. Well configured firewalls and two factor authentication provide a high degree of security. The communication between Visma applications is according to current security requirements and will be updated when needed. Integrations to Visma applications through 3rd party products are out of Visma's control and you need to rely on the documentation and security advise from the suppliers of these components.

Note: Always keep your Windows environment updated with the latest patches (especially security patches). Follow the release notes of your Visma applications and consider patching/upgrading if security issues have been addressed.

Special installation/configuration recommendations

The installation of the Visma Business product line has to be done by a user with administrator rights.

Passwords for administrator users should always have a higher level of complexity compared to normal users.

Visma Business

Visma Business database connection

The recommended way to connect to the database is by using SQL Server authentication with encrypted password in registry. This enables the highest level of security for the Visma Business product line installation.

Visma Zpider

Visma Zpider communication with the web server.

The protocol used in the communication between client (browser) and the Zpider web server is HTTP per default. It is highly recommended to change it to HTTPS after the installation.

User access in general

Access control is an important aspect of GDPR (knowing who has access to which data). In general access control is based on roles/access groups which determine what a user can do.

The recommended way for handling users in the Visma Business product line is by using Visma User Directory for user authentication. It provides the highest level of security by:

- Extensive password policy options; from version 13.00.0 of the Visma Business product line password policies are updated to a higher level of security; after an upgrade to Visma User Directory 13.00.0 or later version all users being part of the **Default password policy** will be upgraded to the **Standard user password policy** (**system user** and **VUDAdmin user** will be upgraded to the **Admin password policy** with even higher complexity requirements). It is possible to reduce the complexity level of both policies but it is not recommended.
- SHA256 password hashing

- With an enabled integration to Visma.net it is possible to use Visma.net login in order to access on premises applications

Note: It is important to set up the **E-mail settings** in Visma User Directory in order to be able to retrieve passwords.

Besides that, it is the responsibility of each company to secure their IT environment (firewall settings, password policies, two factor authentication, permission management, etc…). Please check with your hosting provider if you have any questions about how they secure your environment if you have chosen to use a professional hosting service.

Visma Business

Visma Business access control

In Visma Business there is a second concept on top of roles/access groups. It is possible to restrict what a user is allowed to see in the application by the layouts connected to each user. It is the responsibility of each company using the Visma Business product line to set up the access rights and layouts in a way that the users working in the system don't see information or can't change data which is not intended for their role in the company. With an increasing degree of labor division, it might be needed to separate roles (rights to create suppliers and update bank accounts from the rights to approve payments). Visma Business supports good controls for that kind of setup with the user access conflict table where a company can define which combination of rights should not be assigned to one single user. The user access conflict report (part of the standard reporting package) will show all users which are in conflict with the defined rights. These definitions need to be implemented individually by each company using Visma Business.

Visma User Directory logs all changes to access control. The full history is accessible through the menu **Settings** and **Security log**. If Visma User Directory is not in use then it is recommended to set up the logging for the following tables:

- **User** table
- **User access** table
- **Company group** table
- **Company group member** table

For tracking who sees what in the Visma Business screens/layouts it is recommended (regardless if Visma User Directory is in use for access control or not) to set up logging for the **Layout group** and **Layout group member** tables.

Visma Document Center

Visma Document Center access control

When Visma Document Center is used then an Administrator user in Visma Document Center can change/grant user rights for that user. User data changes are logged in the Visma Document Center event log and are marked with a GDPR_UserDataChanged event type (for the case where Visma Document Center handles that and Visma User Directory is not used).

Visma User Directory

Visma User Directory access control

Visma User Directory provides 4 different roles with limited access in the application. The most powerful role is granted by adding a user to the user group called **VUD superusers**. Being member of that user group provides full access to all functionality in Visma User Directory. After an initial installation only the VUDAdmin user is part of that group.

Visma ERP POS

Visma ERP POS access control

The user administration for Visma ERP POS is only possible in the application itself since Visma ERP POS is not integrated with Visma User Directory.

Visma Reporting

Visma Reporting access control

The user administration for Visma Reporting is mostly done in Visma User Directory. There are two types of roles which need to be considered when giving access to users.

- Server roles
- Company roles

Server roles give a user various functional access to the application itself. The so called company roles grant access to various reports in a reporting package. Company roles are added to Visma User Directory when a new reporting package is deployed.

Visma Zpider

Visma Zpider access control

The user administration for Visma Zpider is only possible in the application itself since Visma Zpider is not integrated with Visma User Directory.

Audit trail

This section covers the necessary setup to establish an audit trail for relevant items.

Visma Business

Visma Business audit trail

Visma Business is logging each record in the database with the user who created it (and date) and the user who last changed (and date) the record. This is not always enough. It is recommended to enable the standard logging in Visma Business for certain changes in the system. For example, it might be useful to log changes on bank account fields (new, change, delete). In theory every field changed in the system can be subject for the standard logging functionality in Visma Business. However, it is not recommended to enable logging on transaction tables like order or order line table or voucher tables because this will decrease the overall performance. The standard logging functionality in Visma Business requires log definitions in the **Change log definition** table. The log itself is stored in the **Company change log** table for entities belong to a certain company and in the **System change log** table for entities belonging to the system database like the **User** table.

Admin users like the **system user** in Visma Business or the **VudAdmin user** in Visma User Directory should only be used for the initial setup of the system. After that only newly created users for actual people with proper rights assigned to them should be used for further updates in the applications. This will ensure that all changes are logged with a user-name matching the person who performed the changes. For Visma User Directory it is enough to add these users to the user group called **VUD superusers**. From version 13.00.0 of Visma Business product line it will be possible for administration work in Visma Business to create a normal user for administration purpose and elevate the rights to the **system user** in order to perform steps which are not allowed for normal user accounts. This can be done in the **User** table in Visma Business setting **Login as system** in the **Modules** field. Only one user at the time can be logged into Visma Business with system user rights, either by log on as the user "system" or another user with the option **Login as system** set. For some operations the **System supervisor** flag must be set. This is the same as for the **system user**.

Note: Do not share user-names and passwords with anybody once the system has been set up and is ready for production use.

Visma Document Center

Visma Document Center audit trail

- Visma Document Center is logging each record in the database with the user who created it (and date) and the user who last changed (and date) the record.
- Bank account changes are logged in the event log and are marked with a GDPR_BankAccountModified event type.
- Organization number changes are logged in the event log and are marked with a GDPR_OrgNrModified event type.
- Document archived files that are deleted are logged in the event log and are marked with a GDPR_ArchivedDocumentDeleted event type.

Visma User Directory

Visma User Directory audit trail

The following is covered by the security log

- Add companies
- Add/remove users to user group
- Add/remove company to company group
- Grant/remove server roles
- Grant/remove company roles

Besides that there is server side and client side logging in the `ProgramData` folder on the hard-drive where the server and client are running.

Visma ERP POS

Visma ERP POS audit trail

The following has been added in version 13.00.0

- Mandatory employee selection for users (also for the default Admin during initial setup)

- Logging of password changes, whether done by a user for himself or by the administrator for another user
- Logging of role assignment changes

Visma Reporting

Visma Reporting audit trail

There is server side and client side logging in the `ProgramData` folder on the hard-drive where the server and client are installed. You can set logging level based on your needs in **Reporting Server configuration** and **Reporting Web configuration** files.

Visma Zpider

Visma Zpider audit trail

There is no log tracing changes in Visma Zpider. Access to specific companies is handled in the ERP.

Shared folders

It is the responsibility of each company running the Visma Business product line to align the access to shared folders on the local network with the access in the Visma applications. For example if a user should not have access to invoice information in Visma Business then this user should not have access to the folder on the local network where PDF copies of these invoices are stored.

3rd party integrations not using standard interfaces

This section covers integrations to Visma Business not using VBS or BIG.

Some third-party applications are not using Visma Business Services (VBS) or BIG in order to update the ERP database. They use direct database updates in the Visma Business database. It is highly recommended that these applications get their own SQL Server user which has limited rights matching only the operations which are required for the 3rd party product.

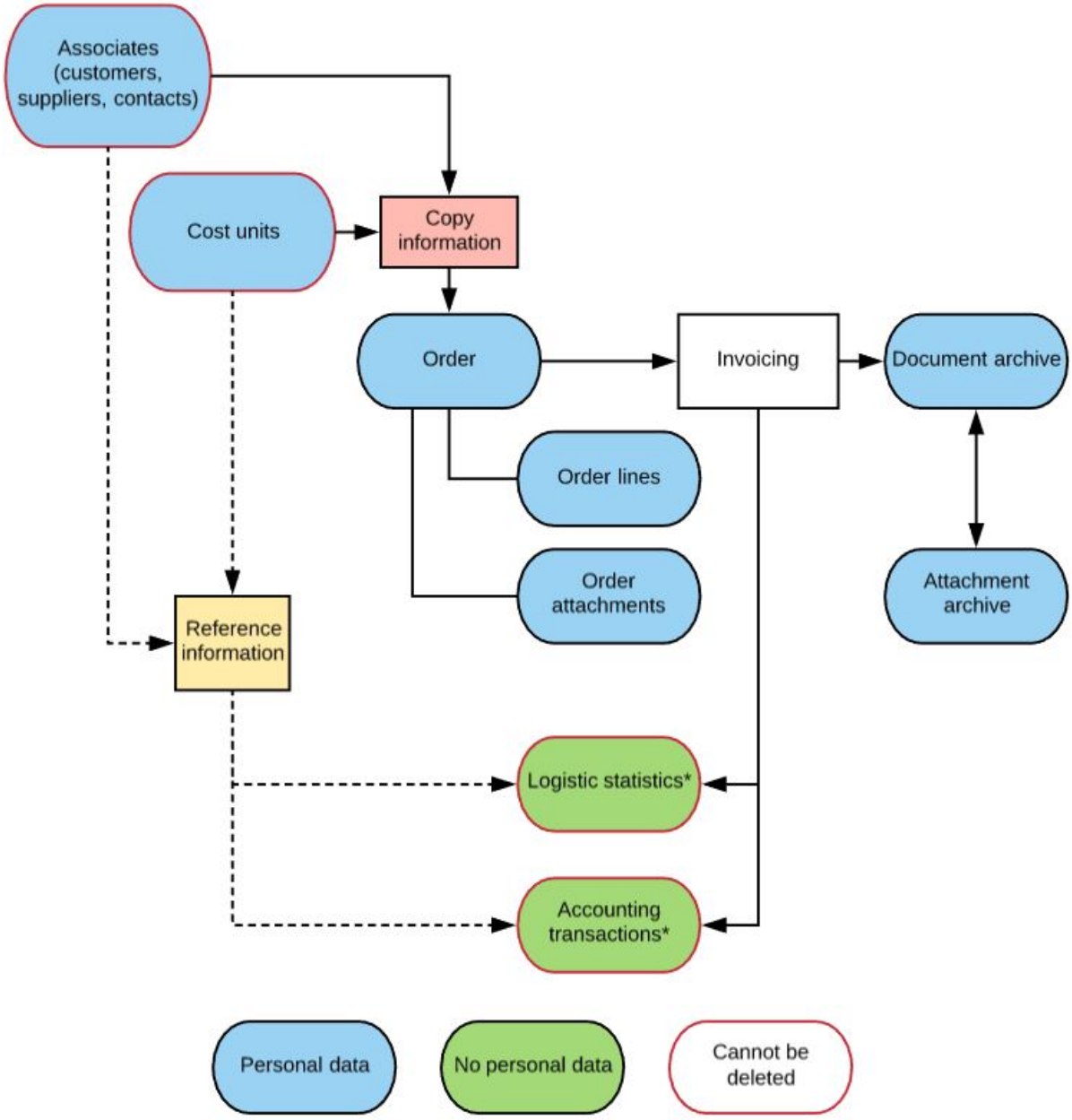
Note: Do not use the **sa user** because this user has full database access and if there is a breach in a third-party application then somebody might get full access to your databases.

Appendix

Additional information and visualisation.

Entities containing personal data

Visualisation of entities containing personal data per design and the relations between these entities.



How to deal with security related incidents

This section summarizes what should be done concerning security and integrity of the system.

In order to have appropriate responses to suspicions behavior or security breaches of your system it is important to know as much as possible about how your system is deployed and how it is configured. Here you can find guidelines for *Secure setup of the Visma Business product line* (see page 9)

There are two levels of logging which should be reviewed.

- Logs outside the applications are usually stored under `C:\ProgramData\Visma` as text files. These logs cover in a typical Visma Business product line installations the following applications:
  - Visma Business
  - Visma Document Center
  - Visma Reporting
  - Visma User Directory
  - Visma ERP POS

- Visma On Premises Gateway

The main purpose of these files is to trouble shoot applications in case services are not starting, or processings are failing across them.

> **Note:** Each application might have several logs/folders covering different sub-services of them.

- Logs inside the applications
  - **Company change log** and **System change log** in Visma Business;

    > **Note:** These logs are always empty until log items have been defined; it is up to each company using the Visma Business product line to establish the appropriate items for them

  - The **Event log** in Visma Document Center provides log-items for the most important activities (including GDPR relevant changes).
  - The **Security log** in Visma User Directory is tracking all changes regarding role assignments.
  - The **Activity reporting** in Visma ERP POS covers role changes, password changes.
  - Visma Reporting does not have any log within the application.
  - In general changes to any record in the database will always be stamped with the time and the user who performed the change.

  The main purpose of these logs is to provide an audit trail for changes to the various entities in the applications. A thorough review of these logs is recommended if suspicious activities have been spotted/reporting.

Plans for the upcoming releases

Version 13.00.0 of the Visma Business product line will make it easier to follow the new regulations regarding data protection. However based on customer feedback and best practises we will continue our process in optimizing Visma applications when it comes to data deletion and data anonymization.

For the second half of 2018 we are planning to introduce better features for data deletion/anonymization in Visma Business which go far beyond what GDPR requires from a company. One of the main features will be to move old accounting and logistic transactions from an existing active customer to a new customer number (generic customer no for all old transactions). That will enable the deletion of a certain customer once all transactions have been moved to the generic customer number (considering the bookkeeping legislations).

The security log in Visma User Directory will be extended to cover more changes in the permanent log. The visualisation will also be improved. It will also be possible to export the current role assignment from Visma User Directory into a CSV file.

Visma ERP POS will deliver improved password management functionality.

Security and best practices for setting up product line environments will evolve over the upcoming years as more and more data processing moves into the cloud. These kind of changes are evaluated during the planning phase of every new release. This guide will be continuously updated with each new version of the Visma Business product line.