GDPR Guidelines Visma Global

GDPR Guidelines Visma Global 1

1.0 What is GDPR? 3

1.1 Who does the GDPR affect? 3

1.2 How does Visma prepare for GDPR 3

1.3 What constitutes personal data? 3

2.0 General GDPR aspects 4

2.2 Data subject rights which affect functionality in our software 5

2.2.1 Right to Access 5

2.2.2 Right to be Forgotten 6

2.2.3 Data Portability 6

2.2.4 Privacy by Design 7

2.2.4.1 Proactive and preventive 7

2.2.4.2 Privacy as the default setting 7

2.2.4.3 Privacy embedded into the design 8

2.2.4.4 Full functionality 8

2.2.4.5 End-to-end security 8

2.2.4.6 Transparency 8

2.2.4.7 Respect for user privacy 9

2.3 Use of data in Visma Global 9

2.4 Storage of data with personal information 9

2.5 Data exchange across applications 12

2.6 Data exchange/sharing 13

2.7 Requests for removing personal data 13

3.0 Recommended GDPR setup of Visma Global 14

3.1 Installation and database connection 14

3.2 Access control 14

3.2.1 User access and security 14

3.2.2 Extended access control 15

3.2.3 Access control with VUD 15

3.2.4 Visma Document Center access control 16

3.3. Audit trail 16

3.3.1 Set up of changelog 16

3. 3.2 GDPR - Personal data removal report/log 19

3.3.3 Visma Document Center audit trails 20

3.4 Shared folders 20

3.5 3rd party integrations not using VAF SDK 20

1.0 What is GDPR?

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations 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.

1.1 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.

1.2 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

1.3 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 Global product line in order to set up the system in a way to support the new requirements according to GDPR. However, Visma Global 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 Global 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 Global with the following products:

- Visma Global
- Visma User Directory
- Visma Reporting
- Visma Document Center
- Visma ERP POS

Visma Global or Visma Document Center are often connected with Visma.net cloud services like Visma.net AutoInvoice, Visma.net 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/

The products described in this document are intended for use in a so-called on premises environment (locally installed software on Windows operating systems). That means each company using Visma Global needs to assume ownership and responsibility for the environment where the software is installed and run, and each company has the ultimate responsibility for meeting the requirements of GDPR. Visma's role is to provide software which makes it possible to comply with the regulations and provide guidelines and tools to make it easier for a company to follow GDPR.

2.0 General GDPR 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 Global can be found below.

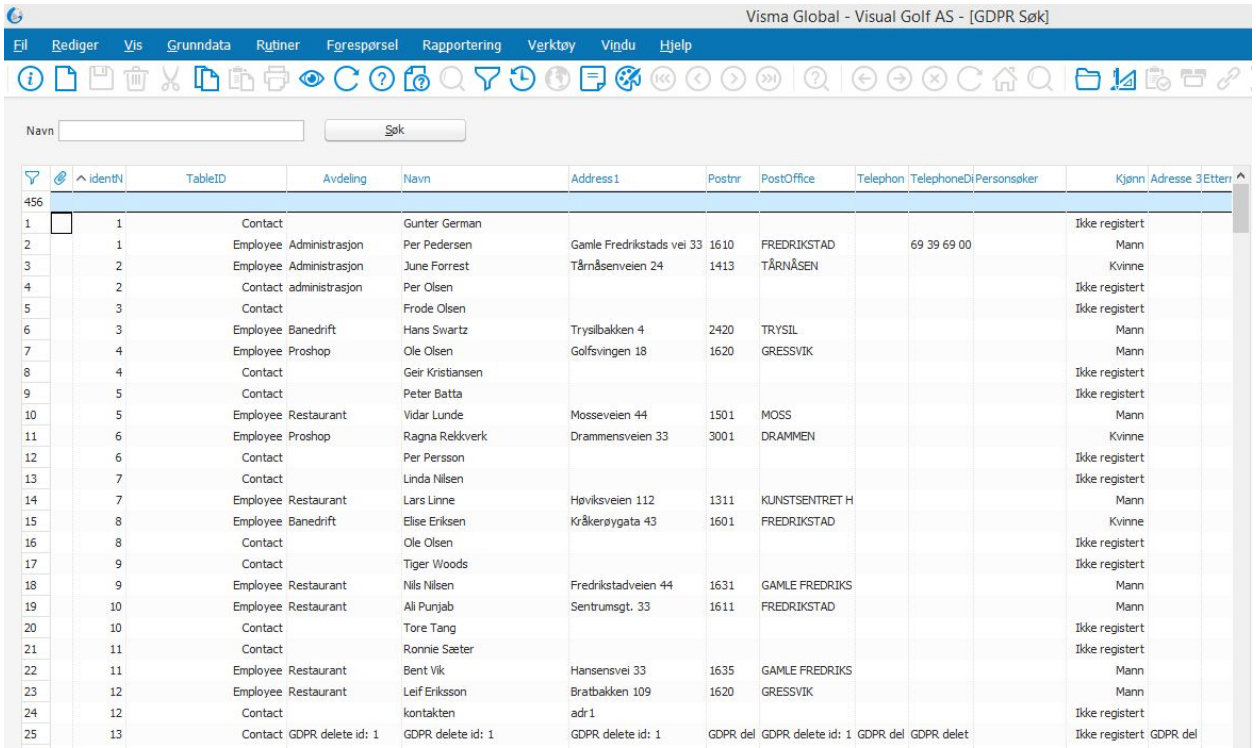
2.2 Data subject rights which affect functionality in our software

The following list summarizes the most relevant rights for a data subject in the context of Visma Global.

2.2.1 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.

In Global you can provide a copy of the personal data in an electronic format (PDF), from the GDPR report, (v. 13.00), found under the menu Tools > GDPR > Search window. You can search for the name of the person in question and write out a report to email/PDF or printer.

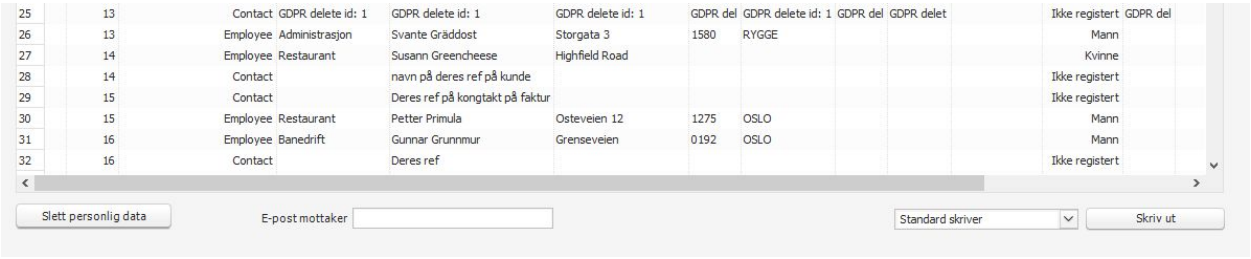


	identN	TableID	Avdeling	Navn	Address1	Postnr	PostOffice	Telephon	TelephoneDi	Personsøker	Kjønn	Adresse 3	Etterr
456													
1	1	Contact		Gunter German							Ikke registert		
2	1	Employee	Administrasjon	Per Pedersen	Gamle Fredrikstads vei 33	1610	FREDRIKSTAD		69 39 69 00		Mann		
3	2	Employee	Administrasjon	June Forrest	Tårnåsenveien 24	1413	TÅRNÅSEN				Kvinne		
4	2	Contact	administrasjon	Per Olsen							Ikke registert		
5	3	Contact		Frode Olsen							Ikke registert		
6	3	Employee	Banedrift	Hans Swartz	Trysilbakken 4	2420	TRYSIL				Mann		
7	4	Employee	Proshop	Ole Olsen	Golfsvingen 18	1620	GRESSVIK				Mann		
8	4	Contact		Geir Kristiansen							Ikke registert		
9	5	Contact		Peter Batta							Ikke registert		
10	5	Employee	Restaurant	Vidar Lunde	Mosseveien 44	1501	MOSS				Mann		
11	6	Employee	Proshop	Ragna Rekkverk	Drammensveien 33	3001	DRAMMEN				Kvinne		
12	6	Contact		Per Persson							Ikke registert		
13	7	Contact		Linda Nilsen							Ikke registert		
14	7	Employee	Restaurant	Lars Linne	Høviksveien 112	1311	KUNSTSENTRET H				Mann		
15	8	Employee	Banedrift	Elise Eriksen	Kråkerøygata 43	1601	FREDRIKSTAD				Kvinne		
16	8	Contact		Ole Olsen							Ikke registert		
17	9	Contact		Tiger Woods							Ikke registert		
18	9	Employee	Restaurant	Nils Nilsen	Fredrikstadveien 44	1631	GAMLE FREDRIKS				Mann		
19	10	Employee	Restaurant	Ali Punjab	Sentrumsgt. 33	1611	FREDRIKSTAD				Mann		
20	10	Contact		Tore Tang							Ikke registert		
21	11	Contact		Ronnie Sæter							Ikke registert		
22	11	Employee	Restaurant	Bent Vik	Hansensvei 33	1635	GAMLE FREDRIKS				Mann		
23	12	Employee	Restaurant	Leif Eriksson	Bratbakken 109	1620	GRESSVIK				Mann		
24	12	Contact		kontakten	adr1						Ikke registert		
25	13	Contact	GDPR delete id: 1	GDPR delete id: 1	GDPR delete id: 1	GDPR del	GDPR delete id: 1	GDPR del	GDPR delet		Ikke registert	GDPR del	

2.2.2 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.

In Global you can fulfill the right to be forgotten in the GDPR report found under the menu Tools > GDPR > Search window. When the conditions for erasure are being fulfilled you can search and mark the person or persons you want to delete the personal information from, and push the delete button. The routine will then remove the personal information from the record and replace it with "GDPR deleted". The removal of personal info will be logged with a timestamp and the user that was responsible. Furthermore a receipt of the deletion of data can be sent to the requestor.



2.2.3 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.

In Global you can fulfill the right for the data subject to receive the personal data in an electronic format from the standard csv export routine, found under the menu Tools > Export data > CSV file. From most tables you can also copy content to Excel.

2.2.4 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.

Visma Global development seeks to provide the tools for the data processor to be compliant, and have focus on the Privacy by Design concept, throughout the development cycle, within the following areas. (based on the Norwegian Data Inspectorate`s checklist for Privacy by design).

2.2.4.1 *Proactive and preventive*

The Global development team is a part of an "ISO 9001:2015" certified organization. This ensures that we have an approved Quality Management System in place with a defined set of policies, processes and procedures required for planning and execution. This means that before every release of a Visma Global main version we have done sufficient amount of testing, piloting and stabilizing to proactively prevent any security issue to arise when customers implement the new version.

We recommend the data controller using the system to train their personnel, (data processors), and implement a quality management system that includes procedures to proactively protect the privat people's personal information in the system.

2.2.4.2 *Privacy as the default setting*

Through default access control Visma Global ensures that only authorized identifiable named users have access to the data. The access control system allows user to have different levels of access and different areas of access. In addition the functionality with "extended access control" can be implemented that gives the data processor partly access to data or a range of data in a specified table. (See the Visma Global user manual for further information)

We recommend the system administrator to set up a strong access control regime, with strong password authentication and AD, (Active Directory), control.

2.2.4.3 Privacy embedded into the design

Visma Global does not by default store any sensitive data, but the system allows users to enter data of sensitive nature if they choose to do so. The entering of data of such nature is the sole responsibility of the data processors of the system and can not be controlled by the vendor of the system.

2.2.4.4 Full functionality

Due to the access control and licensing, users are only granted access to data or modules that is relevant and necessary for data processing. Trough logs and changelog it is possible in the system to see who did what and when.

2.2.4.5 *End-to-end security*

Visma Global has a Server-Client architecture, and a user needs to have appropriate credentials and rights in order to access any of its functionality (this is ensured by access control policy and licensing). In reference to ABV (Avtale om bruksrett og vedlikehold), or "Terms Of Service', The customer is recommended to use the latest database technologies with the appropriate encryption methods and security.

The "End-to-end security" concept also consists of not only the access rights and entering of private information in the system by the processor, but also the protection of the data during the daily processing, and at the end secure removal or deleting of data when the data is no longer relevant or necessary to keep.

From v. 13.00 of Visma Global there is new GDPR functionality, described previously, that enables the processor of removing the personal information in the system in a secure way when the data is no longer mandatory or necessary to keep according accounting laws or other purposes.

2.2.4.6 *Transparency*

In Visma Global, the system administrator can utilize functionality like "changelog" to track changes done by data processors in the system. This functionality is later described in this documentation. (Section: Secure setup of Visma Global)

2.2.4.7 Respect for user privacy

Visma Global as an on premise system does not provide the access right to private persons to control, edit or delete their personal data. However from Global v. 13.00 a new report can easily be produced, by the data processor, to send an e-mail/pdf to the person who wants to know what kind of information we have in the system directly related to their name, to ensure that the information is correct or request the right to be forgotten. (See also section "request to remove personal data below")

In general no sensitive data is required or stored in the database in order to use the full functionality of the system by the authorized data processors.

2.3 Use of data in Visma Global

The Visma Global application 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 application 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 the application, it also applies to free text fields or new fields/tables added to the database by design studio.

The tools provided by Visma for GDPR compliance rely on a standard use of the system. According to the standard use of Visma Global, there is no sensitive data stored in the system. However integrations such as Visma Lønn could transfer sensitive data related to employees, to be booked on the general ledger account in Global. If this is a relevant scenario we recommend processors of the two systems to identify the sensitive data, and make sure that the information only is accessible to authorized personnel or data processors that need to have access to this data to complete their daily tasks.

If a company engages in large scale processing of sensitive personal data 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 will be handled for that type of data.

2.4 Storage of data with personal information

Visma Global could store personal data in the following locations:

- SQL Database:

- Visma Global company database (default naming: CompanynameGlobalData)
  - Default tables that could contain personal information:

Description	Sql Table name
Customers	Customer
Suppliers	Supplier
Contact persons	Contact
Employees	Employee
Documents (Attachments - No control of the GDPR content)	Document
Order (Only Name)	Order
Ordercopy (Only Name)	Ordercopy
Attachments incoming (No control of the GDPR content) - Incoming accounting documents - Incoming documents	
Memo	Savednotes

  - The databases can be extended with Design Studio; 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 “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

- Visma User Directory database
  - User information
- 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.
    - ERP POS database
        - User information
        - Customer information

- Locally stored files could contain personal information
    - Log files are stored in ProgramData folder on the server and client machines for all products
    - In Visma Global, it is possible to do several file path settings; these will determine where the files will be stored locally.
        - PDF documents
        - Memo files
- Visma Document Center stores a minimum of personal data including user's name and email address plus supplier contact names and email addresses. Login credentials are stored either in Visma User Directory or in Global and not in Document Center.
    - Visma User Directory and ERP POS store personal data in form of user information.

    - 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\)

- Cookies used for embedded pages
    - Visma.net pages
    - Visma Reporting Web client

Storage of backups:

- It is recommended to backup data produced by Visma applications on a regular basis. This kind of service is usually offered by companies who are hosting Visma Global 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.

2.5 Data exchange across applications

The products mentioned in the introduction part (Visma Global 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 connected to the locally installed products like Visma.net AutoPay, Visma.net AutoReport, Visma.net AutoInvoice, Visma Storage, etc...
- 3rd party applications (off-the-shelf products) or custom-made applications
    - using the API of the locally installed Visma Global
    - 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 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 Global products and 3rd party applications. You need

to contact the vendors and verify that they are secure and in line with GDPR regulations. This also applies to custom made integrations which add or retrieve data from Visma Global.
Data can also be transferred via export from Visma Global 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.

2.6 Data exchange/sharing

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.

2.7 Requests for removing personal 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). The 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. Contacts, customers, suppliers (in special cases), employee and user records 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). If documents have been sent via email then these documents will be archived in the “sent” folder in your email client. These documents are also part of GDPR regulations.

3.0 Recommended GDPR setup of Visma Global

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 Global installation. 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 Visma Global 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 system.

3.1 Installation and database connection

The installation of Visma Global has to be done by a user with administrator rights.
The recommended way to connect to the database is by using SQL Server authentication with encrypted password. This enables the highest level of security for Visma Global installation.
Passwords for administrator users should always have a higher level of complexity compared to normal users.

3.2 Access control

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.
In Visma Global there is a second concept on top of that. With Extended access control it is possible to restrict what a user is allowed to see in the application. It is the responsibility of each company using Visma Global to set up the access rights 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). These definitions need to be implemented individually by each company using Visma Global.

3.2.1 User access and security

In the Access control register you enter users with access to the system. Users are defined and linked to the correct Access group. Each Access group can then be given the required access level to the various parts of the system.

Access Group:
Select the Access group that you want to process on screen. The settings are saved by Access group for later maintenance. The first user to be created during installation is automatically defined as the Administrator.

Roles:
For every single role there will be a series of routines/screens to which you can provide access. When you place the cursor at the top of the roles tree, all routines will be displayed in the table on the right-hand side. If you select a role further down the tree on the left of the screen, the routines that belong to the role will be called up on the right.

Restricting access to the use of routines:
On the right of the screen you can restrict access by selecting the Full, Read and None options.

> **Full:** Provides access to create, modify and delete the selected routine.
>
> **Read:** Only provides access to read, *not* to create, modify and delete the selected routine.
>
> **None:** Blocks access to the routine.

3.2.2 Extended access control

In extended access control you can define which Access groups have access to which parts of the tables.

3.2.3 Access control with VUD

Another way for handling users in Visma Global is by using Visma User Directory for user authentication. It provides the highest level of security by:

- Extensive password policy options
- 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

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 User Directory logs all changes to access control. The full history is accessible through the menu Settings and “Security log”.

3.2.4 Visma Document Center access control

When Visma Document Center is integrated to Visma Global users must be defined in the ERP. Then an Administrator user in Visma Document Center can change/grant user rights for that user.

- For Visma Global customers, if Visma User Directory is in use then users must be handled in the VUD API.
- 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).

3.3. Audit trail

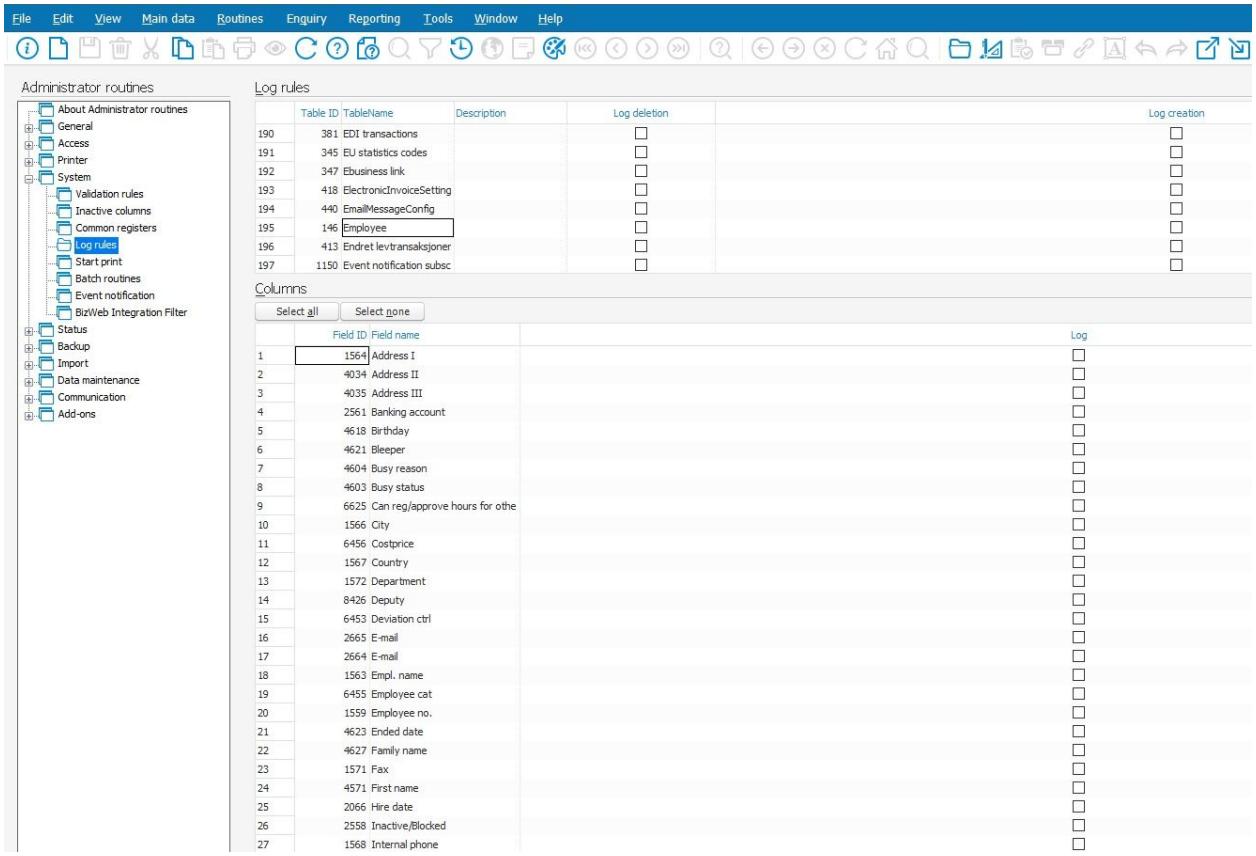
Visma Global is logging each record in the database with the user who created it (and date) and the user who last changed (and date) the record. This is not always enough. It is recommended to enable the logging functionality in Visma Global for certain changes in the system. For example, it might be useful to log changes on bank account fields (new, change, delete). In theory, every field changed in the system can be subject for the logging functionality in Visma Global. 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.
Administrator users in Visma Global 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 system. This will ensure that all changes are logged with a username matching the person who performed the changes.

3.3.1 Set up of changelog

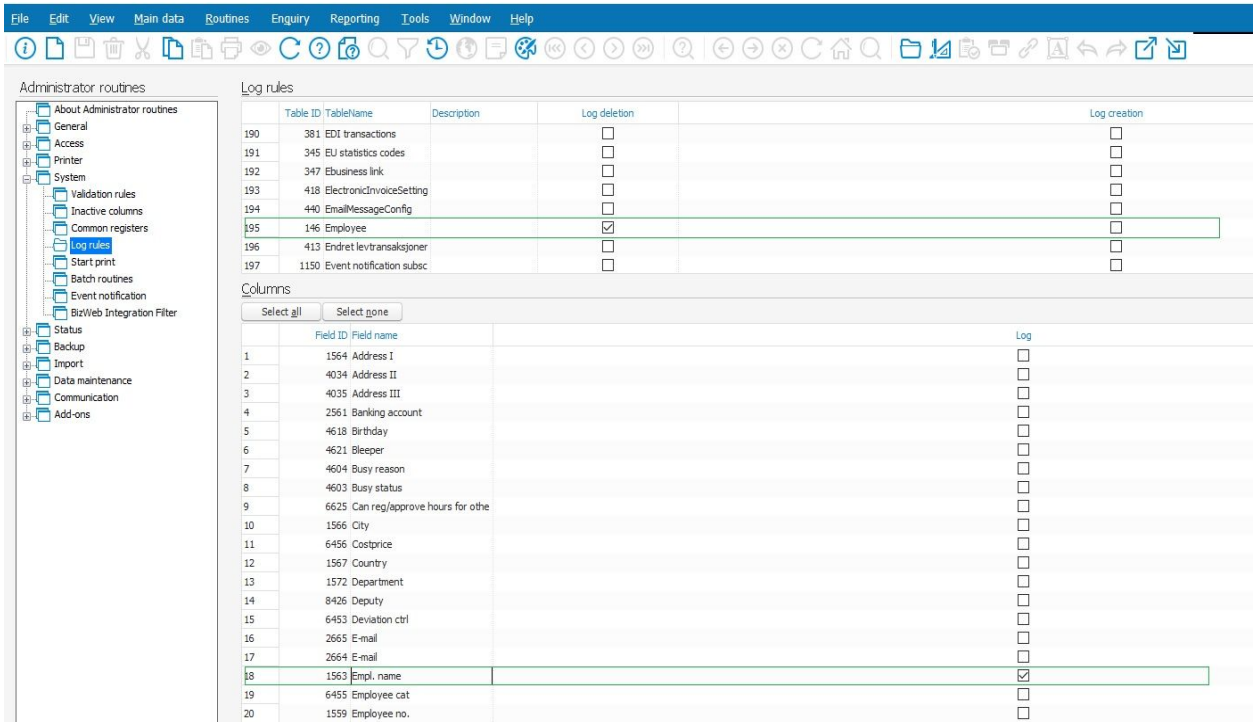
This functionality can be found in Visma Global under the menu Tools > Administrator routines > System > Log rules.

By accessing this the user will notice a list of tables that are in Visma Global; the user can set the application to log deletion and/or creation for one of the tables or to log deletion/creation of one or more of their fields by clicking the respective check-boxes.

Here is an image of the form:

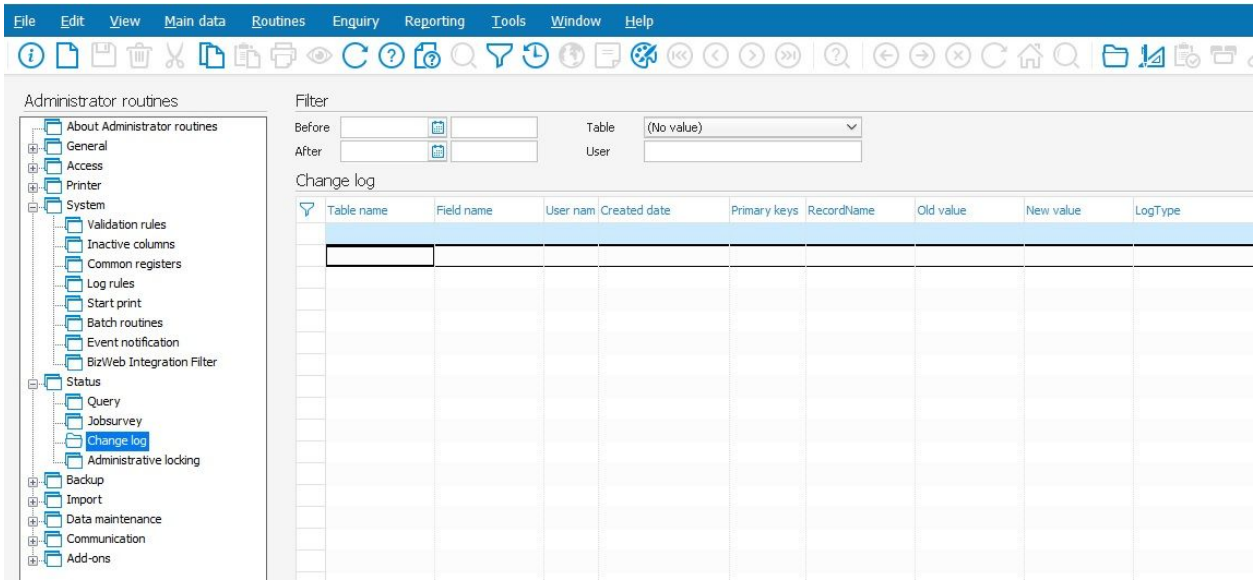


As an example, the user can choose “Employee” table to log deletion of an ‘employee name’ by clicking “log deletion” checkbox in the first table and then by clicking “log” checkbox for “Empl. name” field in the second table:



After this has been set up the changes that were logged by the application will be found under the menu Tools > Administrative routines > Status > Change log.

This form contains a header that helps the user to filter the changes and a grid containing the records of what has been changed by that moment (accordingly to the filters set up in the header), as in the image that follows:



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

3. 3.2 GDPR - Personal data removal report/log

This can be found under the menu Tools > GDPR > Search.

This functionality as described previously allows users in Visma Global to search for a name of a person and have displayed all the personal data regarding that person in a table. The result of the search can be printed or exported as a PDF file and handed to the respective person (or sent by email).

The functionality allows removal of the personal information in the records found about the specified person within the boundaries of the law. Also there is a log of the names of the deleted records and who deleted the record at what date and time. This can be found under Tools > GDPR > Log.

3.3.3 Visma Document Center audit trails

- 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.

3.4 Shared folders

It is the responsibility of each company running Visma Global 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 Global then this user should not have access to the folder on the local network where PDF copies of these invoices are stored.

3.5 3rd party integrations not using VAF SDK

Some third-party applications are not using VAF.net/VAF SDK in order to update the ERP database. They use direct database updates in the Visma Global 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.
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.