8MAN

Access Rights Management. Only much Smarter.

WHITEPAPER GDPR

How to secure your organization with 8MAN

TABLE OF CONTENTS

Management Summary 2

1. Background information on the GDPR 3

2. Central GDPR requirements 4

Article 5: Principles for the processing of personal data 4

Article 32: secure processing 4

3. Requirements of Access Rights Management 5

Article 5: Implicit Requirements 5

Article 32: Implicit Requiremens 5

4. Implementing central GDPR requirements with 8MAN 6

5. Steps for the implementation of a GDPR conform security architecture for your organization 8

5.1 Nominating Data Owners and assigning resources to them 8

5.2 Locating and centralizing files containing personal data 10

5.3 Reducing access rights to files containing personal data 10

5.4 Monitoring directories and groups with the help of Security Monitoring 12

5.5 Involving your organizations security roles automatically through reporting 12

5.6 Maintaining an overview of directories containing personal data 13

5.7 Removing directory access rights when employees move departments or leave the company 13

6. Questions to ask your IT and business departments 14

7. About 8MAN 14

8. Contacts 15

MANAGEMENT SUMMARY

The General Data Protection Regulation (GDPR) is on its way, bringing with it a number of new requirements for your organization. This document is designed to help you implement important aspects of the GDPR and understand how to properly prepare your organization for the future. The GDPR's mandate is to protect personal data. On the one hand, it focuses on the protection of consumers, but it is also invaluable in setting standards for the protection of public organizations and private corporations.

Specifically, implementing the GDPR will protect your organization from Data-, Information- and Knowledge theft. Ultimately you should treat digital data in the same way as protecting sensitive paper documents in a safe. By not taking the appropriate measures, this data can be easily copied and sold. Experts agree that protecting sensitive company data is a worthwhile endeavor necessary to safeguard your organization's unique competitive advantage.

Chapter 6 covers several test questions. Try answering these in your company to see how quickly IT and business departments can find accurate and appropriate answers. If you are currently operating without a professional access rights management solution, we would be happy to issue you with a complimentary test license for our 8MAN software solution.

Please contact us. We are always ready to show you, how your organization can benefit by using 8MAN.

Stephan Brack, CEO

Matthias Schulte-Huxel, CSO

1. Background information on the GDPR

The GDPR was put in place by the European commission to regulate the processing of personal data. The directive became effective on 25.05.2016 and will become official law by 25.05.2018. This replaces the previous data protection guideline of 1995 (95/46/EG). As a supranational EU law the regulation applies immediately and does not require any additional national legislation.

By implementing these measures commission is prosecuting data protection violations with increased pressure. An expression of the seriousness of the EU initiative are the new fines associated with a violation. Whereas previously penalties ranged from 50.000-300.000 Euro, the EU is now able to fine organizations up to 20 Million Euros or 4 percent of the organization's annual turnover (GDPR Art. 83 Abs. 4 und Abs. 5).

The data protections laws protect natural persons, located in the EU protection from unauthorized use of their personal data and regulates companies and institutions worldwide in the processing of this data.

Personal data are characterized by a connection between a person and another person, thing, or event. Constitutive for personal data is the possibility of connecting the data to a specific person. Examples of personal data include car license plates, account numbers, social security insurance numbers, registration numbers, Email, and IP addresses. The determining factor in applying these regulations is not the location of the company, but rather the physical location of the individual person whose data was collected.

2. Central GDPR requirements

The GDPR is extremely complex. In total it contains eleven chapters, that are subdivided into 99 articles. Experts are attributing the most relevant impact to article 5 and article 32. These represent the most important additional requirements compared to previous data protection guidelines.

Article 5: Principles for the processing of personal data

(1) Section e) personal data must be processed in a way that ensures an appropriate level of security for personal data. This includes the protection from unauthorized access and undesired loss, destruction, or damage, through the appropriate technical and organizational means (Integrity and Confidentiality)

2) The responsible party must ensure the adherence to § 1 and must be able to document and prove this.

Article 32, secure processing

(4) Both the responsible and the processing party must take steps to ensure that all reporting employees who have access to personal data only process and analyze this data upon explicit request from a responsible party, unless they are legally required by law of the (European) Union and their member states.

3. Requirements of Access Rights Management

Articles 5 and 32 imply a number of access rights management requirements for your company.

Article 5: Implicit Requirements

1. Ensuring data security and integrity: Resources that contain personal data must only be accessible to trustworthy individuals. Additionally, all folders must be subject to continuous monitoring. This ensures, that all copying and modification processes are documented and an accurate history is available at all times. In case of a security incident, both IT and business departments can access the relevant information and determine the appropriate measures.

2. Documentation of access rights: Especially, the accountability requirement of article 5, paragraph 2 states that data processing institutions must account the for exact access and permissions history of each directory.

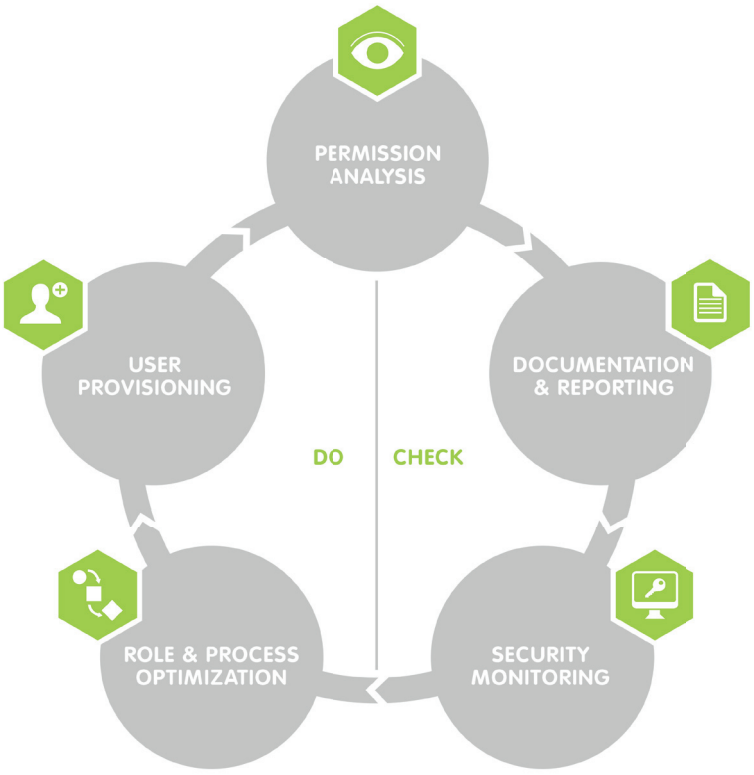
3. Maintenance of access rights situations: The joiners, movers, and leavers process (including the life cycle of a user account in your company network) requires both IT and business departments to maintain an overview of all access rights, and make changes very quickly. Data theft most often occurs during the leavers phase. At this point, business departments need to have already removed the employee's permissions to security critical directories.

Article 32: Implicit Requirements

4. Introducing Data Owners: The GDPR demands clear responsibilities when processing personal data. In this context, introducing the role of a data owner is absolutely central. Data Owners are managers that protect data within their departments. They know exactly, which directories must be protected and which employees require access. The introduction of new roles such as data owners also requires new processes of collaboration and documenting shared activities and responsibilities.

4. Implementing central GDPR requirements with 8MAN

8MAN includes five central disciplines. Together they make up a clear and easily implementable system to achieve GDPR conform access rights management.



PERMISSION ANALYSIS
Displays a comprehensive overview of the access rights situation to resources in your organization.

DOCUMENTATION & REPORTING
Records any access rights activity in our logbook and creates audit proof reports

SECURITY MONITORING
Monitors security relevant actions in Active Directory and on your file servers.

ROLE & PROCESS OPTIMIZATION
Shortens your access rights management process and involves only the most important actors.

USER PROVISIONING
Sets rules for the creation of new user accounts, the provisioning of rights and the editing of account details.

One of the central tasks of fulfilling GDPR requirements is **Permission Analysis**. 8MAN shows the access rights situation in your network in both directions. You can either select a resource that includes personal data and be shown, who has access to it, or you can be shown all access rights of a selected user. With this knowledge, the requirement (1), „Creating data security and integrity", can be quickly implemented.

The access rights situation, activities on protected directories, as well as the process of assigning access rights is fully documented in well-structured reports in **Documentation & Reporting**. Reports can be automatically sent for specific directories to selected roles within your organization. In this way, the requirement of documenting all access rights is fulfilled automatically.

Besides access rights considerations, the actual handling of personal data is also very important. Our **Security Monitoring** deepens the level of security and capture activities within directories, that contain personal data. Beyond this, the AD analysis also shows changes made outside of 8MAN. In this way, temporary group memberships and the resulting, often uncontrolled permissions, become immediately transparent. 8MAN informs you proactively via the alerts feature, if someone attempts to manipulate the rights and membership of a sensitive security group.

With **Role & Process Optimization** 8MAN offers a sequence of best practice processes, that are essential for GDPR conform access rights management. The process for controlling and maintaining access rights to personal data must be clearly defined within the organization. Role & Process Optimization provides the required framework. One of the central aspects of this policy is the conception of a data owner role: Requirement (4) „Introducing data owners". Managers decide on and manage the access rights situation in their departments and determine, who should have access to personal data. Through periodical recertifications, the data owner can add and remove permissions, or leave them unchanged, even without any specific IT knowledge.

Even during quarterly recertifications, the ad-hoc care of the access rights situation remains an important requirement. If an employee leaves your company, his access to sensitive information and other company data needs to be removed at an early stage. This is performed by the data owner or administrator, via drag & drop in **User Provisioning**. Requirement (3): Maintenance of the access rights situation.

5. Steps for the implementation of a GDPR conform security architecture for your organization

The following chapter shows you the most important steps required to achieve a GDPR conform access rights management. You can find the documentation for this service in our User Guide.

5.1 Nominating Data Owners and assigning resources to them

To improve IT security for personal data, you must firmly put in place the required measures and policies. The goal is to decentralize the security competence in your organization. Do this by nominating a data owner for the areas where personal data is used and processed. Generally, these include procurement/finance, sales and of course HR.

DATA OWNERS, DATA SECURITY OFFICERS, AND AUDITORS

Typically, CEOs assign the responsibility of data ownership to department managers. They know which data in their department is worth protecting and who should have access to it.

The data owner is the „First Line of Defense". He reports to the data security officer, who in turn provides advice on rights and responsibilities regarding the handling of sensitive data („Second Line of Defense").

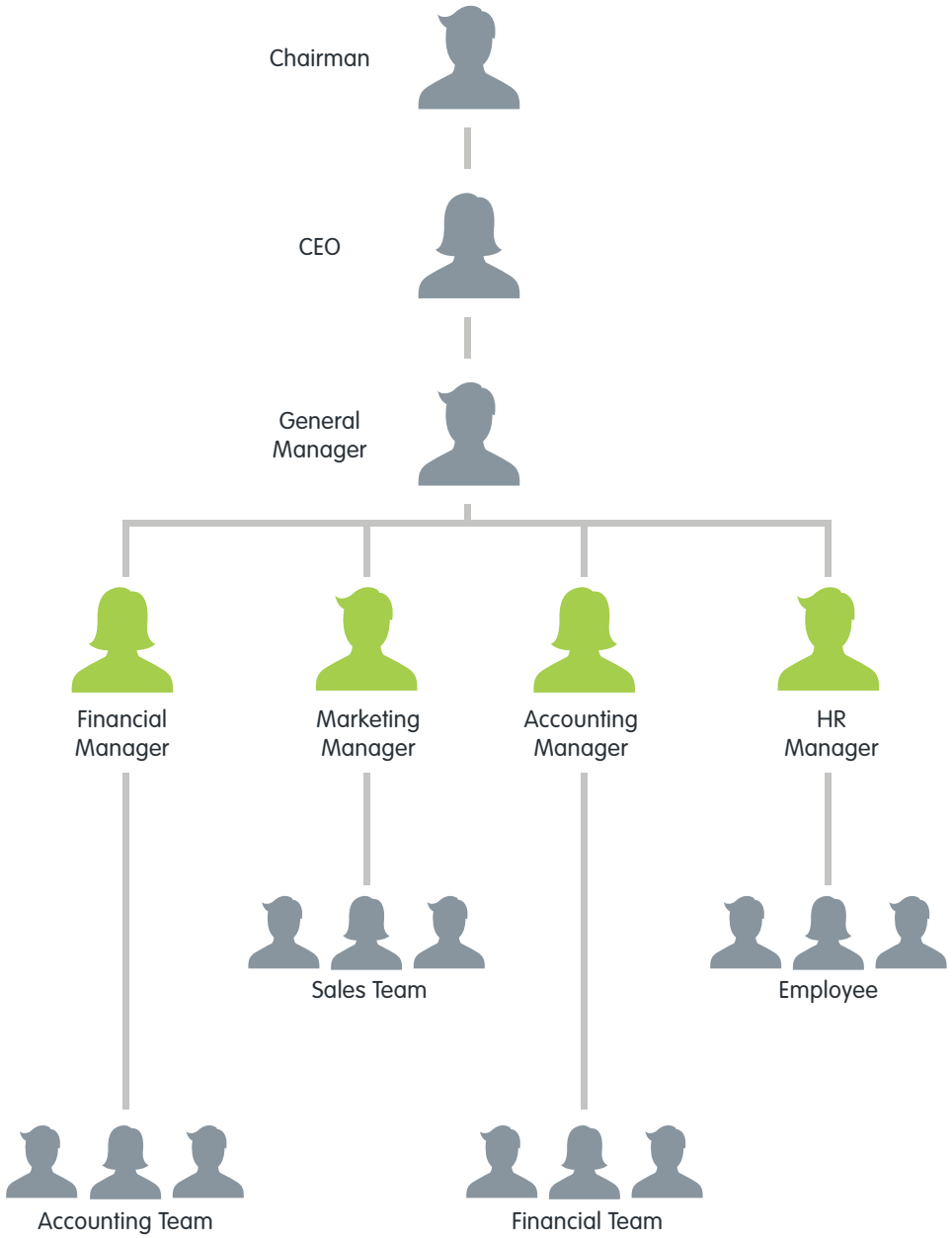
The „Third Line of Defense" is typically an internal or external audit. Both data security officers as well as internal auditors should be regularly informed about the current access rights situation. 8MAN also enables you to give these security roles read only access to 8MAN, providing them with an instant overview of current permissions (**D013**). (see image on page 9)

8MAN DISCIPLINE: ROLE & PROCESS OPTIMIZATION

Shortens your access rights management process and involves only the most important actors.

Required Steps:

- ✓ **D002** Define Data Owners and allocate resources
- ✓ **D003** Assign the administration of folder rights to a Data Owner (Decision Makers)
- ✓ **D013** Apply an 8MAN Account for a specific Security Role or Data Owner


Chairman
CEO
General Manager
Financial Manager
Marketing Manager
Accounting Manager
HR Manager
Sales Team
Employee
Accounting Team
Financial Team

5.2 Locating and centralizing files containing personal data.

In the next step, every data owner takes inventory of their assigned resources and locates all files containing personal data. If these are located in different directory tree structures, we recommend centralizing these within one branch. (see image on page 11)

5.3 Reducing access rights to files containing personal data

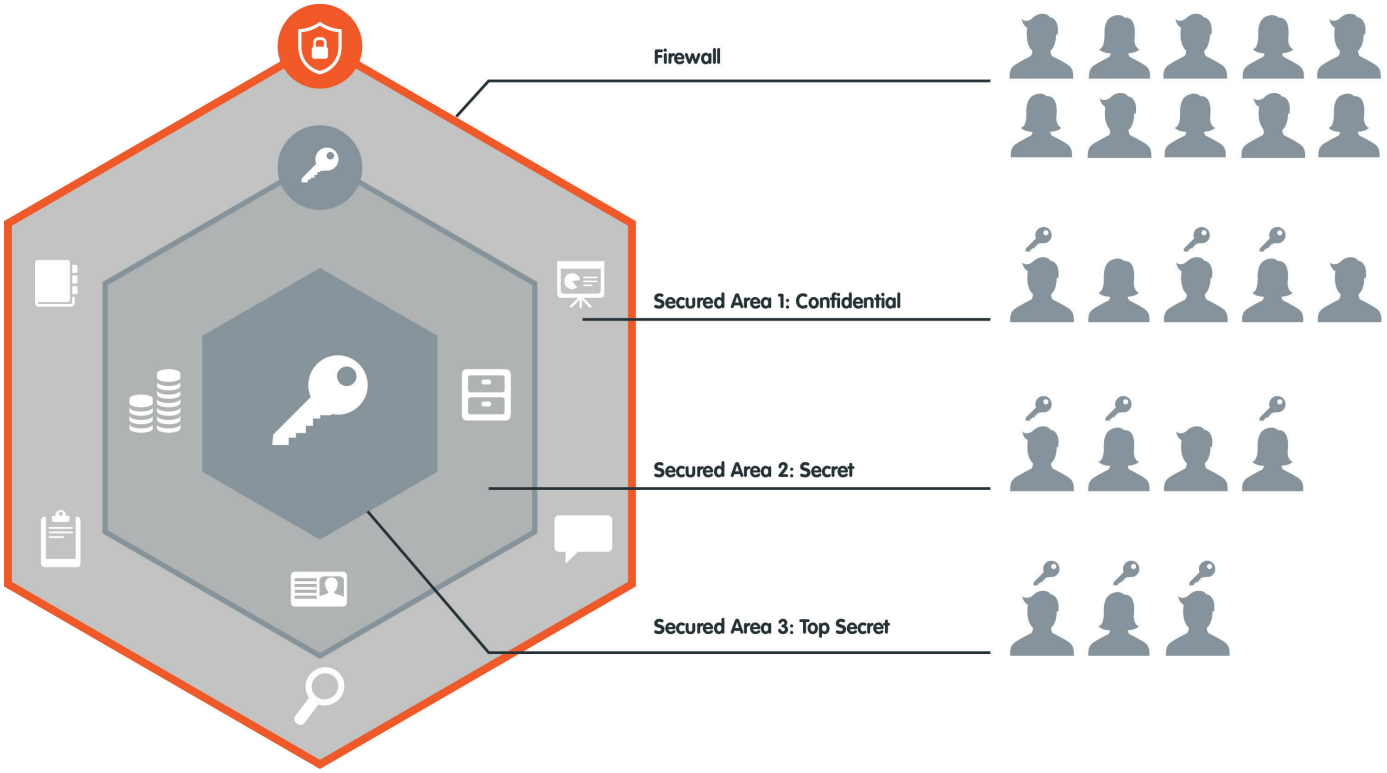
Create an AD security group and use it to provide access to all users requiring access to a security-critical directory (**E001**). Then identify any multiple access paths and remove these so that the only remaining access is provided by membership in the previously created security group (**E017**). Next you should remove any permissions of people who do not necessarily require access to personal data to perform their role (**E015**). Here, the „Principle of least Privilege" applies. It states that access to security relevant data should only be granted on a need to know basis.

8MAN DISCIPLINE: USER PROVISIONING

Sets rules for the creation of new user accounts, the provisioning of rights and the editing of account details.

Required Steps:

- ✓ **E001** Create a user account
- ✓ **E017** Remove multiple access paths to folders
- ✓ **E015** Change folder permissions



Personal data belongs to the section „protected area 2".
Only a small number of employees should have access to this area.

5.4 Monitoring directories and groups with the help of Security Monitoring

The next step is implementing Security Monitoring. If your personal data is stored on your file servers, we recommend analyzing actual access to directories regularly (**C009**). You can then send reports to data security officers and internal auditors. This way you can automatically involve the required security roles in your organization. Your AD Group can be secured via the alerts feature (**C005**). If anyone makes changes to this group, then data owners, data security officers and CEOs will automatically be informed via E-mail alert.

8MAN DISCIPLINE: SECURITY MONITORING
Monitors security relevant actions in Active Directory and on your file servers.

Required Steps:
- ✓ **C009** Identify the access to sensitive data
- ✓ **C005** Alerts: Create, edit and delete alarms for AD groups

5.5 Involving your organizations security roles automatically through reporting

Reports on the current access rights situation or data access to personal data should periodically be provided to the data security officer and/or internal auditor. 8MAN allows you to define reports to specific directories and automatically send these to the responsible parties via E-Mail (**D020**). Services (**B034, B014, C009**) are particularly relevant in this context.

8MAN DISCIPLINE: DOCUMENTATION & REPORTING / SECURITY MONITORING
Records any access rights activity in our logbook and creates audit proof reports /
Monitors security relevant actions in Active Directory and on your file servers.

Required Steps:
- ✓ **D020** Receive Reports automatically
- ✓ **B034** Where do users and groups have access?
- ✓ **B014** Who has access to what?
- ✓ **C009** Identify the access to sensitive data

5.6 Maintaining an overview of directories containing personal data

Permissions to security critical directories must be regularly audited by data owners. The 8MAN recertification feature (**D023**), activated by the Administrator, periodically reminds data owners of their responsibility. In a simple overview, they can quickly verify directory specific permissions and manage these as necessary (**D024**).

8MAN DISCIPLINE: ROLE & PROCESS OPTIMIZATION
Shortens your access rights management process and involves only the most important actors.

Required steps:
- ✓ **D023** Activate the recertification process
- ✓ **D024** Recertificate the current access rights situation

5.7 Removing directory access rights when employees move departments or leave the company

As soon as an employee moves to a different department it requires the immediate removal of departmentally specific access rights. Data owners can easily do this in the 8MAN web interface. When an employee leaves the company access rights to security critical directories should be removed as soon as possible (**E052**).

8MAN DISCIPLINE: USER PROVISIONING
Sets rules for the creation of new user accounts, the provisioning of rights and the editing of account details.

Required Steps:
- ✓ **E052** Removing permissions using the webclient

6. Questions to ask your IT and business departments

1. Where do we store our personal data and who has access to it?

2. Which files does Mr. Smith have access to?

3. Who did what on a directory in a specific time-period?

4. Which are our most important and security relevant AD groups, what do they grant access to and who is a member of them?

5. How am I informed if an AD security group or user account is manipulated?

6. Who can give me a quick and easy to read report about the current access rights situation within my organization?

7. Who is responsible for protecting security relevant directories in their departments?

8. When did we last audit and recertify existing access rights?

7. About 8MAN

8MAN is a leading solution in the field of Access Rights Management (ARM) in Microsoft- and virtual server environments and protects your company from unauthorized access to sensitive data. The 8MAN solution was developed in Germany by Protected Networks. By combining modern functionality and usability aspects with current compliance and IT security standards, 8MAN sets new standards for professional network security and agile IT organization. The 8MAN core disciplines include: Permission Analysis, Security Monitoring, Documentation & Reporting, Role & Process Optimization, and User Provisioning.

HOW TO SECURE YOUR ORGANIZATION

The introduction of 8MAN is not a cumbersome project, but just a quick phone call away. Just set up an appointment and a qualified, certified technician will ensure the proper installation and configuration in your environment. Depending on specific requirements, the installation can usually be completed through remote access quickly and easily.

8. Contacts

Sven Reinhardt
Head of Sales Engineering & Professional Services

+49 30 390 63 45-66
sven@8man.com

Free Webinar Start with a 30-minute overview and see 8MAN in action. Participants can remain fully anonymous amongst each other. At the end of the presentation you can ask questions via chat.

Free Trial Installation Test 8MAN for free with a 21-day trial license. See for yourself how 8MAN provides value and insight to your organization.

8MAN | Protected Networks GmbH

Alt-Moabit 73
10555 Berlin
Germany

T: +49 30 390 63 45 - 0
E: info@8man.com
W: www.8man.com

Author:
Fabian Fischer
Knowledge Manager

+49 30 390 63 45-41
fabian@8man.com