otherside at work

for happy professionals

SECURITY & PRIVACY CONTROLS

OTHERSIDE SOFTWARE B.V.

VERSION	1.4
STATUS	Final
DATE	January 18th, 2023
CLASSIFICATION	Sensitive

powered by fair priced technology

CONTENTS

INTRODUCTION

Otherside Software B.V. (Otherside) attaches great importance to the security of its customers' data, as well as to the privacy rights of data subjects about whom data is collected. The high standards that we set for this are reflected in physical, technical and procedural measures that we impose, adhere to and monitor both internally and also with respect to our suppliers.

In this brochure, Otherside's security approach is broken down into the following subjects:

1. Security:
    a. Embedding information security in the organisation
    b. Logical and physical access security
    c. Functional management, connections and hosting
    d. Monitoring and improvement of security measures & incidents
    e. Software development
    f. Backup & restore procedures
2. Privacy:
    a. Processing agreements
    b. Privacy officer
    c. Data subjects counter
    d. Retention periods
    e. Privacy by design, Privacy by default

This brochure gives you an impression of how Otherside interprets security. If you have other questions then of course please feel free to contact us.

Furthermore, we would also like to draw your attention to the ISO-27001 certificate, which Otherside obtained in October 2012. The management system used by Otherside to manage the risks around the availability and security of Xpert Suite is audited, certified and accredited in accordance with this international standard.

In addition, we are audited annually on a selected set of our privacy & security controls, after which an SOC2 report is issued.

1 SECURITY

1.1 Embedding information security in the organisation

Information security is managed via the ISO 27001certified Information Security Management System (ISMS), registered via the BSI Group under certificate number ISC-077. The administrator of this is the 'Information security officer', the CTO (member of the board) will be end responsible. The management system is an integral part of the (annual) control cycle of the company as a whole:

1. Each year, a risk analysis is performed on the basis of the experiences of the past year and developments within the environment;
2. Based on the risk analysis, improvement plans are drawn up and submitted to the board for approval;
3. After approval, the implementation of these points for improvement is monitored fully by the MT in the managing of the company.

As well as the management system itself, management processes are set up for which responsibilities are separated. Each process has someone with final responsibility who, in consultation with the board, determines when and on what controls take place. Whether or not each person responsible actually tackles his or her role is ultimately verified in the annual internal and external ISO audit. The controls/measures set up, as defined in ISO 27002, are all under management and controlled.

The following management processes have been established:

1. Access management
2. Asset management
3. Backup management
4. Capacity management
5. Change management
6. Compliance management
7. Continuity management
8. Customer management
9. Dataloss and malware protection
10. Incident management
11. Key management encryption
12. Logging management
13. Personnel management
14. Third party management
15. Vulnerability, Patch management & Hardening

Within personnel management, explicit attention is paid to:

1. Awareness about information security; once a year a knowledge session is planned examining the importance of information security for our customers and for the survival of our company. Posters and other visual aids are also used periodically to alert people to the procedures. Examples include the lists by the waste paper bins and the printers identifying which items may and may not be thrown away in them or printed. The personnel manual also contains various guidelines regarding information security and refers actively to the information security policy. In addition to the procedures, the awareness creation actions with regard to information security also emphasise the potential major consequences of any improper handling. These consequences concern the people and customers about whom information is recorded in our systems. The aim of this is not only to motivate employees to follow the procedures exactly, but also always to continue to think critically about whether actions are being performed that can have serious negative consequences for our customers and thus also for Otherside itself.

2. Competences; When someone joins the company and each year thereafter, an active assessment is made of whether the competencies of the individual are in line with the position held or whether any development is required. When competencies are no longer in line with the position, a change of position is a possibility. When personnel changes occur,

an active assessment is made of whether the correct competencies are still present in the company or whether gaps have appeared. In the latter situation, we look at how these competencies within the organisation can be redeveloped or brought in.

3. Integrity; When hiring employees, a number of actions are performed to determine if the person is trustworthy when it comes to working with privacy-sensitive data:
    a. Diploma/reference check;
    b. Certificate of Good Behaviour (VOG) request;
    c. Signing of a declaration of confidentiality;
    d. Customer specific screenings.

4. Active assessment of working in line with information security policy; The extent to which an employee acts in accordance with the information security policy is part of the assessment interview. If an employee does not act properly in this respect, active warnings are given that can result in termination of employment. The self-reporting of any incident caused personally is assessed much less negatively than if another employee reports it. This is to prevent a culture of fear from developing.

1.2 Logical and physical access security

The most important measure is the strict physical and logical separation of the office environment (without customer data except for financial administration) and the production environment (with customer data). For this the following applies:

1. No employee of Otherside has independent physical access to the areas where customer data is stored. This always requires the cooperation of the hosting partner (ProServe) and the approval of the board.
2. ProServe employees can physically access the equipment on which customer data is stored. However, this data is stored on encrypted disks and in encrypted databases, making the customer data unreadable for ProServe employees.
3. The physical access to the office environment is recorded by the facility manager in a key plan and assessed annually. The areas covered in this key plan are: workstations (general), workstation financial administration, server room office environment (no customer data) and archive with administration.
4. The logical access to the office environment is managed operationally by workplace management. Again, a printout of the active directory and the access rights on the various servers are checked annually.
5. The joining and leaving protocol includes a checklist used to verify that all physical and logical access is closed. In addition, the checklist includes a number of other steps regarding the return of equipment and related items.
6. Logical access to the production environment is screened separately.
7. A limited number of employees have access to the production environment. This only if necessary for the performance of their own work.
8. Employees with access are given a personal user name and password, installed certificate and a second factor (time-based token) for an end-to-end VPN connection to the production environment.
9. With an active VPN connection the employee can connect to a dedicated jump host with separate Active Directory credentials.
10. Access to the servers for authorised employees is restricted depending on function. Only the servers necessary for their own work are accessible.
11. Access rights are actively updated in the event of job changes and leavers. The accuracy of the rights assigned is checked annually.
12. Just as for all other users, access to production databases via the web interface is always secured with 2-factor authentication.

The management of the physical and logical access is included in the access management procedure which in turn is part of the ISO27001:2013 certified ISMS.

1.3 Functional management, connections and hosting

Within the Xpert Suite, the customer administrators themselves can define and assign roles to users. Based on these roles, the software determines which changes users may and may not make. The basis of this authorisation is that the role determines what a

user may do while the link to the employee files of the individual user determines for whom this is allowed. Taken together, these authorisations determine whether or not a change is permitted. Of course, in this context, all incoming changes are assessed by the server against the configured authorisations. Administrators can print out an IST matrix of the what authorisations and all the configured roles and have them tested internally (IST vs SOLL).

For the management of the servers on which the software and customer data are located, an employee also needs to be assigned a role defined in the Active Directory. This role assignment is kept up to date and checked periodically for accuracy. The standard windows mechanism is then used to restrict rights. Access to the management environment requires a VPN connection with certificates and 2-factor authentication.

As an additional measure, Otherside has set up a SIEM that collects and analyses both the data traffic and the logging of actions carried out. This allows an additional assessment and active escalation if a user or software component performs 'unusual' actions.

All traffic to the production environment enters via a physical firewall whereby only traffic that has been explicitly opened and thus approved via the change procedures is allowed. The traffic is then routed over a segmented network whereby only the web and connection servers for which it is intended are accessible via the Internet.

Web traffic is always secured via TLS, whereby the TLS settings are tested for known vulnerabilities using external tools. File exchanges take place via TLS or SFTP.

The database servers are not directly accessible and the databases are separated per customer. Stored data is encrypted by means of the TDE mechanism of SQL Server and in addition there is also cell level encryption for medical data entered by company doctors. The cell-level encryption takes place via the application with a customer and application key. Besides that all Virtual Machines are stored on encrypted VMWare VSAN storage.

The data is stored at the following primary locations:

EU Networks *Paul van Vlissingenstraat 16* *1096 BK Amsterdam*	*Dataplace* *Van Coulsterweg 6* *2952 CB Alblasserdam*

Backup information is stored in both the local location as in the remote location.

At both locations, the hardware is managed by sub-processor ProServe. The address of ProServe is:

Proserve BV
Oostmaaslaan 71
3063 AN Rotterdam

The backups are also stored at a separate cage within Dataplace which is not accessible by ProServe nor internal Otherside-employees, unless one-time access is provided by the board of Otherside.

DNS services are provided by a third party, protected by two factor logins and also monitored for changes with an independent external monitoring tool.

1.4 Audits and monitoring of Security improvement measures & incidents

Non-conformities can be established in a number of ways:

1. During the annual internal audit;
2. During the annual external ISO27001 certification audit;
3. During the annual SOC2 audit;
4. As a result of the analysis of a reported incident.

Incidents can be reported by customers or employees or can be the result of a (periodic) audit of a control measure by a responsible contact person.

After a non-conformity has been established, an action plan is prepared. This action plan focuses on the question of what measures are necessary to remedy the non-conformity identified and to prevent it from recurring. A conclusion could be, for example, that the working methods in place are of such a sub-optimal nature that the temptation to bypass them is too great and that therefore modifications are necessary.

In order to monitor whether the measures taken have had the desired effect, for each measure, how and how often its effectiveness should be measured are explicitly defined. The responsible contact persons then implement the measures adopted. During the audit, all controls are checked to see whether this has been done.

Security incidents are discussed in the yearly knowledge session and, if caused by an individual or department, with the employees involved. When it is necessary to inform all employees immediately about security incidents (i.e. earlier than the next annual knowledge session), a news message is sent internally. If a security incident leads to a (potential) data leak, the 'Duty to Report Data Leaks' procedure is followed. Within this procedure, data controllers need to be informed within 24 hours in accordance with the guidelines of the Dutch Data Protection Authority.

The audits are performed a number of times per year:

- Once per year, an internal audit, in which Otherside itself carries out checks on procedures of data controllers within the organisation. The results are discussed internally and improvement actions identified.
- Once per year, an external ISO 27001 certification audit (once every 3 years an official certification and in between times a control audit each year). Based on these audits, a report is prepared and it is decided whether Otherside may retain the certificate.
- Once per year, an SOC2 audit performed by an external certified auditor. The auditor issues a signed declaration of the checks performed and the consequences for customers.

1.5 Software development

Otherside has incorporated Secure Development principles into its development methodology. For each individual change, the impact in terms of security is assessed in accordance with the requirements in the ISO 27001 guidelines. Developers use a checklist for this based on the OWASP top 10 guidelines, ISO27002 controls, NCSC and NIST. For each release, the modified code is reviewed against this checklist and delivered to the Maintenance & Support department. Maintenance & Support then carries out a number of technical and functional acceptance tests, in which the operation of authorisations is tested before the new release goes into production.

At least once per year, an external party is asked to perform PEN tests on the software. The PEN test supplier is changed every 2 to 3 years to ensure a critical analysis. These tests are as of 2023 performed by Intigrity. In addition to the annual penetration test, we are also gradually implementing a full scale bug bounty programme in 2023, so that our complete stack is part of a bug bounty programme in 2024.

We use Sigrid CI for the assurance of Open Source Health and Security Issues in our code.

Secure programming competencies of developers are developed and kept up-to-date with the help of internal and external parties.

1.6 Backup & restore procedures

Data is protected against destruction by a backup process which is performed on customer databases on the past 7 days, 4 weeks (before that for 7 days) and 5 months (before that for 4 weeks) basis (thus effectively for a maximum of the last 6 months). The backups are encrypted and periodically checked by means of restores.

Otherside has set up three backup locations. At the same location as the primary location for a customer, at the secondary location of a customer and at a dedicated cage in Dataplace which is not accessible by ProServe nor internal employees, unless one-time access is provided by the Board. This third location is using Veeam Insider Protection to prevent the possibility to delete the backups from the backup management server.

If the primary location is destroyed, the application will be available on the secondary location. If data is destroyed on both locations the data can be restored from the Veeam Insider Protection backup server and will be up-and-running within the period agreed in the SLA.

2 PRIVACY

Sensitive personal data is processed in the Xpert Suite. This means that the consequences for data subjects can be very great if errors are made in the processing. Ultimately, Otherside's customers are the data controllers for this processing but Otherside, with its procedures and measures, wants to offer a platform on which the controller can easily adhere to legal requirements and data subjects' rights. In doing so, we will direct our customers as much as possible towards a compliant working method.
The additional measures that Otherside has taken within the context of privacy legislation are listed below.

2.1 Risk analysis

As part of the annual risk analysis (part of the ISO 27001 certified ISMS and also audited by the SOC2 auditor), Otherside also assesses whether sufficient measures have been taken to cover privacy risks. In this, Otherside uses the CIP framework whereby the following threats are analysed and, where necessary, measures are taken to mitigate the risks:

- CIP B.01 Inadequate adoption of legislation and regulations
- CIP B.02 Inadequate privacy policy
- CIP B.03 Inadequate organic embedding
- CIP B.04 Processing architecture not properly established
- CIP B.05 Inadequate risk management and PIA
- CIP C.01 Inadequate internal supervision
- CIP C.02 Inadequate access to data processing for data subjects
- CIP C.04 Duty to Report processing and data leaks not followed
- CIP U.03 Inadequate quality management
- CIP U.04 Inadequate security
- CIP U.05 Inadequate information provision

Many of the risks are already covered by the existing security measures. The additional measures arising from the risk analysis are described below.

2.2 Processing agreement

Otherside enters into a processing agreement with all the customers who use its software. This agreement has been tested to ensure compliance with the relevant privacy legislation (in any case at least the GDPR). A standard processing agreement can be obtained from Otherside.

2.3 Data Protection Officer and privacy & security team

Otherside has put in place a Data Protection Officer and a privacy & security team. This privacy & security team consists of representatives from all parts of the organisation who potentially come into contact with customer data (consultants, support, IT management). In this consultation, all ongoing improvement actions, incidents and risk analyses are discussed, thus ensuring an integral monitoring of the security. The Data Protection Officer has been appointed to supplement the impact in this consultation of improvement actions, incidents and risk analyses with consequences for data subjects.

The Data Protection Officer of Otherside is:

Joyce Uittenboogaard
E: joyce.uittenboogaard@othersideatwork.nl
T: 06-30228142

2.4 Data subjects counter

Otherside has set up a counter for the data subjects which they can turn to with their questions. The basic rule is that a controller (i.e. the customer of Otherside) must communicate with the data subjects. But if this is not possible, Otherside wants to be accessible to data subjects and support them where possible in resolving any problems. The counter can be reached via:

E: loket.betrokkenen@othersideatwork.nl
T: 073-6159950

Information about the counter is also available on the Otherside website. https://www.othersideatwork.nl/

2.5 Retention periods

The data recorded in the Xpert Suite is subject to very different retention periods (for example, an employer must delete an absenteeism record within 2 years of the person concerned leaving the company while an occupational health and safety service must sometimes keep it for up to 40 years). Otherside has added functionality to its software that can be used as a customer to determine for themselves which periods should be used in which situation. This data, however, can still be present in the old versions of backups for 6 months. After that, the data is permanently deleted / destroyed.

This backup period is of this length due to long-running cases. Sometimes users are very late in discovering incorrectly deleted data. The rights of data subjects also include the obligation to retain data. Because backups are not operationally comprehensible, Otherside uses this period in weighing up the right to data destruction on the one hand against the right of retention on the other.

2.6 Privacy by design and privacy by default

In the software design process, Otherside applies the following principles:

- When making a design, compliance with privacy legislation and the consequences for the data subjects are always included in the analysis;
- If a user has not made a choice for a particular setting then we use the strictest privacy settings (privacy by default);
- If users appear to be diverging from legal obligations then they always need to provide a reason for doing so (e.g. login without 2FA);
- At all points where the software can support users with regard to privacy-compliant operation, Otherside will try to provide a solution which is as user-friendly as possible, so that users follow this compliant working method as far as possible (e.g. not only SMS as 2FA, the Data Safe, DialoogXpert);
- The software supports the establishment of legal bases for processing for the purpose of supporting the data controller.

Of course, Otherside cannot guarantee that every user of the Otherside software works in compliance with applicable laws and regulations. The demonstration of this remains with the controller.