Otherside at Work B.V.

Report on Controls at a Service Organization Relevant to Security Availability and Confidentiality (SOC 3) – Type III Report

For the Period first of January 2021
to thirty first of December 2021

January 27th 2022

Table of Contents

Section 1: Otherside at Work B.V.'s management statement 3

Section 2: Assurance Report of the Independent Service Auditor 4

Attachment A: Organization Overview and System Description 6

A.1 Overview of the Organisation 6
A.2 The principle service commitments and system requirements 11
A.3 Control Environment Elements 12
A.4 Risk Assessment 17
A.5 Information & Communication 18
A.6 Monitoring 18
A.7 Business Processes 19
A.7.1 System development 19
A.7.2 Hosting & monitoring 19
A.7.3 Support and maintenance 20
A.7.4 Incident management 21
A.7.5 IT office management 21
A.7.6 Supplier management 21
A.7.7 Personnel management 22
A.7.8 Compliance management 22
A.7.9 Continuity management 22
A.8 Management control 22
A.9 Complementary User entity controls 23
A.10 Complementary Subservice Organization Controls 23

Appendix B: Service obligations & mandatory compliancy laws and regulations 25

Section 1: Otherside at Work B.V.'s management statement

We are responsible for designing, implementing, operating, and maintaining effective controls within Otherside at Work B.V's Software as a Service system throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Otherside at Work B.V's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Otherside at Work B.V's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Otherside at Work B.V's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment A.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We use subservice organization(s) Proserve B.V.'s to perform hosting Services. The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Software as a Service system also indicates the complementary subservice organization controls assumed in the design of Otherside at Work B.V's controls. The description does not disclose the actual controls at the subservice organization

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Otherside at Work B.V's controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents Otherside at Work B.V's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Otherside at Work B.V's controls.

We assert that the controls within the system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Otherside at Work B.V's service commitments and system requirements were achieved based on the applicable trust services criteria.

January 27th, 2022
Otherside at Work B.V.

D.P.J. Benders
CEO

R.A.A. van der Sanden
CTO

Section 2: Assurance Report of the Independent Service Auditor

1. Scope

We have examined accompanying assertion titled "Management Statement" (assertion) that the controls within Otherside at Work B.V's Software as a Service system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Otherside at Work B.V.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

2. Sub-service organizations

Otherside at Work B.V uses subservice organization(s) Proserve B.V. to perform hosting services. The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed and operating effectively. The description of the boundaries of the system of Software as a Service system also indicates the complementary subservice organization controls assumed in the design of Otherside at Work B.V. controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

3. Objectives at the user entity (Complementary User Entity Controls).

The description of the boundaries of the system (attachment A of this report) indicates that certain applicable trust services criteria can be achieved only if complementary user-entity controls contemplated in the design of Otherside at Work B.V.'s controls are suitably designed and operating effectively, along with related controls at the service organization. The description presents Otherside at Work B.V.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Otherside at Work B.V.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls

4. Service organization's responsibilities

Otherside at Work B.V is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Otherside at Work B.V service commitments and system requirements were achieved. Otherside at Work B.V. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Otherside at Work B.V. is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

5. Responsibility of the service auditor

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We conducted our assurance engagement in accordance with Dutch Law and the International Standard on Assurance Engagements Standard 3000, 'Assurance Engagements other than Audits or Reviews of Historical Financial Information' established by The International Auditing and Assurance Standards Board (IAASB). Those

standards require that we plan and perform our engagement to obtain reasonable assurance to express our opinion. We have complied with the independence and other ethical requirements of the Code of Ethics ('Reglement Gedragscode') issued by NOREA, the Dutch IT-Auditor institute, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior. The firm applies the NOREA Standard on Quality Control (Reglement Kwaliteitsbeheersing NOREA – RKBN), and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Otherside at Work B.V service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Otherside at Work B.V's service commitments and system requirements based the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

6. Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

7. Opinion

In our opinion, management's assertion that the controls within Otherside at Work B.V's Software as a Service system were effective throughout the period January 1, 2021 to December 31, 2021, to provide reasonable assurance that Otherside at Work B.V's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

January 27th, 2022

Alex Klaassen

Drs. Alexander E. Klaassen RE CIPP/E CIPM

Managing Partner NewDay IT Risk & Assurance Services B.V.

Attachment A: Organization Overview and System Description

A.1 Overview of the Organisation

Otherside at Work is a fast-growing SaaS-provider in the Netherlands, Belgium and Sweden. Its software has over 80.000 active users. Otherside at Work focusses its SaaS to support businesses with handling privacy-sensitive data, while in the same time making sure that this data is available when necessary (and when it's allowed). On the SaaS-platforms users can cooperate to execute the business operations while maintaining compliancy.

Otherside at Work's offering is currently focussed on Corporate health management (Dutch: "bedrijfsgezondheidszorg").

Software

XPERT SUITE PLATFORM
Basic functions of the flexible and integrated platform for corporate health management and social security: • Absence, "ziektewet" and "WGA" in one system • Platform vor dynamic and adaptive workflows, with different tasks for different situations • Tailored userportals for different usergroups (also usable on tablets and smartphones). Examples: employerportals, (former) employee portals, claim manager, service provider employee, etc. • User roles and rights configurable to great detail, alsof or service providers with thousands of customers. • Library with standard (but adjustable) workflows for WvP, ZW, WGA • Possible to add prevention-workflows, medical examinations, vaccinations, PMOs • Library with standard management information reports for absence, frequent absence, process, compliancy, financial losses, etc. • Standard UWV-forms, maintained by Otherside at Work • Integration with MS Word for designing document formats • Structured UWV decision administration for WAZO, ZW, WGA, IVA, Wajong, no-risk etc. • Retention periods configuratble per type of file with (semi-) automatic data clean-up. Safe communication within the Xpert Suite: • Safe communication & e-coaching through secured messaging within Xpert Suite • Scanning of documents, photo's, video's directly into the employee file without storing on local device. • For service providers: work in accordance with the AP guidelines by using the Datavault. Employees are separate but safely integrated with your own dataset. Employee data will only be shared if there is a demand for care. Integrationplatform • Enterprise Service Bus (ESB) with standard connectors to external parties (HR, UWV, ARBO, Insurers, CRM and financial) • Single Sign-On based on SAML2

- Standard integration standards (SIVI, XML, SOAP, REST-API, CSV)
- Make your own data exchange based on SFTP (CSV/XML/XLS)
- Dashboarding, monitoring integrity checks

Flexible application management

- Make your own workflows, task triggers, documents, forms, roles, rights

Multifactor authentication

- TOTP (ie Google Authenticator)
- SMS
- Yubikey

Modules	Functionaliteit
Medical files	Support your medical users with a medical case-file, managing your consults, examinations and customer-reporting.
Digital Signing	Users can approve document with an SMS code or a digital signature. This method of digital signing has been approved by the UWV for your casemanagement file (including 'Plan van Aanpak').
Forms	A flexible questionnaire management module to let non-users fill in extra data. Can for example be used to calculate insurance premiums, perform medical intakes, etc. Results are directly visible within the case file.
Scheduling	Flexible online agenda for many users, including support for customer self service, productivity-reports, SMS reminders, etc. Also includes 2-way data exchange with MS Exchange and Google Calendar.
Financial Control	Supports the financial side of social security: calculate additions and subtractions to employee benefits (due to absence), calculate and maximize the compensations from the UWV, directly fill your ledger account with the right amounts, and create reports for providing insights in possible future claims. • Import salary-data from your own Salary/HR software. • Structured administration of UWV decisions and your response to it. • (Dagloon)berekeningen • Import UWV payment specifications • Start appeal or review procedures
No-risk	Automatic digital verification of social security benefits for new employees (LKV and No Risk): • Standard digital questionnaires (maintained by Otherside) • With reminders for non-responders • When employees start their employment or when their first absence due to illness starts • Automatic processing of results and workflows for claiming possible benefits

Contract Management	Complete module for managing different kind of service models, customer contracts, discount-models, dynamic fee's, price indexations, automatic invoicing for both subscription fee's as well as billable unit prices or hourly fee's with the correct VAT-percentages. It's also possible to manage your service catalogue and easily manage all settings for a large number of customers: workflows, labels/styling and split invoicing employers or insurers. Also possibilities for automatic time registration, gain insights in billable and non-billable hours, all hours traceable to customers, projects, activities, costcenters. Integrations possible with multiple accounting software solutions (Exact, Twinfield, Accountview, Afas, etc).
Project Management (optional with contract management)	Fully integrated project administration tool for managing your budgets and invoicing with multiple subprojects. Also includes possibility to manage project members in detail to prevent misuse of budgets.
Insurance policies and contracts	Extendid registration of insurance contracts for a lot of insurance-types (illness, WGA Hiaat, WGA excedent, etc). Policies can be the source of service-model subscription and workflows as well as different labels/stylings/offerings in the market. They can also be used to calculate burden of claims for the different actors. Participant registration per insurance contract, with automatic or manual inclusion as well as manual exclusion. This module is usefull for unsurers and their proxies and can interface with both ANVA and CCS.
Wage related policies (optional with insurance policies and contracts)	With the wage related policies module, occupational disability insurers can automate claim management for their customers. The Xpert Suite is the customer portal for receiving claims as well as calculating the financial result of the received data so that claim specifications can be automatically generated and communicated through a privacy proof portal to customers. The Xpert Suite also generates payment files for approved claims. It's also possible to automate communication to employees to be compliant with pension-regulations. The Xpert Suite will automatically trigger and generate the necessary communication to all participants of the specific insurance policies. Finally, this module also supports the yearly settlement of insurance premiums by using intelligent online questionnaires. After approving the results an automatic settlement is calculated, added to the customer file and sent to the customer.
Provider management	Within the Xpert Suite a customer can manage its preferred suppliers for interventions and the products they offer. These providers can be used in workflows to do cost effectiveness calculations for the specific case. On a higher level this data can be used to show effectiveness of providers and their products.

Datastreams	Automatic files (CSV, Excel or XML) with which you can easily analyse all the data registered by your users in the Xpert Suite. Data files in the form of facts (like absence due to illness, task execution, generated documents) and dimensions (like employers, employees, users, etc) so different BI-tools can easily be connected and used. These can easily be used in toools like PowerBI, Qlik, Tableau, etc. You get the files of your data and extensive descriptions of the data with showcases so any data-analist can start using these files. All the dashboards you want without necessary assistence from Otherside at Work. Freedom to use your data.
Security Management	With the Security management module it is possible to detect security events within the Xpert Suite. These events can be configured to scenario's you want to monitor. You can now pro-actively monitor events like: - Making a privileged account - Adding and removing a user within 24 hours - A blocked account which isn't deblocked within 5 days Add a lot of extra security management to the Xpert Suite to be extra sure the highly confidential data is still secure.
Video-consults	Extension of the scheduling module which adds the possibility to start a video-consult directive from your agenda. Also provides a digital waiting room for clients.

Markets, products and services

Otherside at Work delivers the Xpert Suite (or VerzuimXpert) to large corporates (1.000+ employees), (proxy's of) absence insurers and health & safety service providers.

<u>(Proxy's of) Absence insurers</u>

For these customers the Xpert Suite is the solution that:

a. Provides a client portal on which customers can make claims related to absenteeism
b. calculates which claims the insurer must pay to its customers based on the insurance policy, absence reports and wage data of the customer.
c. Handle the formal assessment of claims with complete tracking & tracing of the calculations and corrections when necessary
d. Automate claim assessment
e. Securely communicate payment specifications to the customers through the client portal
f. Analyse which provider handles controls of claim expenses best

Over 300.000 active employee files are being managed by these (proxy's of) absence insurers daily.

<u>Service providers</u>

For these service providers, the Xpert Suite is a complete ERP solution combined with a collaboration platform, with which the service providers can:

a. Provide a client-portal
b. Communicate and streamline orders and questions from customers to internal employees
c. Configure and monitor workflows to follow-up on these customer calls
d. Have privacy-compliant filing of all privacy sensitive data for which the deliver health services
e. Manage and plan the resources (health care professionals, rooms, etc)
f. Automate their financial flows (contract management, invoicing)
g. Provide insightful management information to their clients and its own management on results that are achieved as well as whether or not the designed process is executed properly.

Over 1.600.000 active employee files are being managed by these service providers daily in Belgium and The Netherlands.

Large corporates

Large corporations have large financial stakes in managing the health of their own employees. In The Netherlands they are obliged to be the insurer of employee income for 2 years (after an employee reports sick) and can choose to increase this period to 12 years (in return for lower employer's contributions to the collective insurance of sick employees). Therefor they actively monitor its corporate health and its service providers.

a. The Xpert Suite supports large corporations with this, by offering a solution that:
b. Supports managing and monitoring every employee that reports sick
c. Collect compliant files of these employees while they are absent to limit risks for extra costs
d. Streamline work processes associated with absenteeism: internally and externally (ie by sending messages to third parties (insurers, UWV, health & safety service providers, etc)
e. Provide insight: where costs are being made and which interventions would most likely limit the risks of extra costs
f. Make sure you optimize the possibilities provided by social welfare laws to limit costs
g. Improve the employability of the workforce by involving lower management

For customers in Sweden and Belgium there isn't an 'income providing' obligation that lasts as long as in The Netherlands, but employers do have the obligation to facilitate the health & safety of their employees. Managing these efforts is largely similar to The Netherlands.

Over 600.000 active employee files are being managed by these major corporates daily.

Data

Within the Xpert Suite personal data is being processed. Customers determine exactly which data and data of which individuals will be processed as well as which users will have access to which (parts of) the data and for which period retention is set.

But in general the datatypes contain:

- General personal data of employees:
    - Social Security Numbers, Name, Address, contacct details, employment details (function, departments, FTE, etc).
    - Health-related data:

- Absenteeïsm-related data
- Casemanagement data (notes, documents, tasks etc.)

- User-data:
    - Name, e-mail, phone number (for 2FA), actions performed within the Xpert Suite and technical logging data (moments of logging on and off etc).

Nature of the processing:

- Collecting and storing the data through manual input, SFTP / webservice processing
- Back-ups
- Signal users to add to/change the data.
- Encrypting the data for storage and transport
- Removing the data (through user-input)

A.2 The principle service commitments and system requirements

Otherside Software, as a software supplier for the Xpert Suite, wants to be known as the system and the partner to which you as a data controller entrust the processing of medical personal data. We want to ensure that our customers (in their capacity as data controllers from the GDPR/AVG) can optimally fulfill their responsibilities and that we have set up the procedural and technical security for our own processes according to high standards appropriate to working with this kind of special personal data.

Otherside at Work wants its services to be characterized by:

1. Reliability & continuity- The procedures and measures of Otherside at Work must ensure that risks are minimized and that incidents are responded to adequately (and transparently for those involved).

2. Controllability- Otherside at Work wants to be transparent in its working methods around information security, so that clients have insight into the measures taken, and that they can fulfil their role as 'data controller' for data processing in accordance with legal requirements. The customer must be able to perform an audit in relation to information security at all times, which Otherside at Work passes with flying colours.

3. Being up-to-date & aware - Policies, procedures, work instructions and other measures are periodically evaluated internally to remain effective in the changing IT world. Employees are also regularly stimulated to be aware of risks and current procedures.

To ensure that Otherside at Work BV has security that meets Otherside at Work BV's vision and values, Otherside at Work BV has designed and implemented an Information Security Management System (ISMS).

Otherside at Work BV's ISMS and security policies were developed based on the ISO/IEC 27001 and ISO/IEC 27002 standards and provide employees with the guidelines on how Otherside at Work BV manages security related to its own activities. The policies set strategical goals for information security. The ISMS provide policies based on information security risk and compliance requirements. Where appropriate and effective in its day-to-day activities, Otherside at Work BV' is process orientated, with processes being based on ITIL (IT Infrastructure Library).

A.3 Control Environment Elements

Otherside at Work's control environment reflects the position taken by the management, its Directors, and others concerning the importance of controls and the emphasis given to controls in its policies, procedures, methods and organizational structure. The following is a description of the key elements of Otherside at Work's control environment related to supporting the services described within this description.

Integrity and Ethical values

Otherside at Work is committed to doing business in a transparent and fair way. We don't abuse a strong position just to maximize our own short-term profit. With both our customers and our suppliers we want to work together in a sustainable way (for all parties involved). This is reflected in the type of employees that are hired and the long-term relations we have with both customers and suppliers.

HR policy

The ethical values we support are also part of the way we treat our employees. We go for a long-term relationship and let our employees focus on creating customer satisfaction in the best possible way. This also means not literally doing what a customer asks, but finding out what the underlying problems are and solving that problem.

Within personnel management, explicit attention is paid to:

- Awareness about information security; knowledge evenings are held several times per year 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.

- 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.

- **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:
    - Diploma/reference check;
    - Certificate of Good Behaviour (VOG) request;
    - Signing of a declaration of confidentiality;
    - Customer specific screenings.
- **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.

Organizational structure

Both directors of Otherside at Work have the ultimate responsibility for overseeing the policies of Otherside at Work. They are both still actively involved in Otherside at Work's operations and quality assurance processes. This also improves the open culture in which problems and incidents are reported to the highest levels so that the company as a whole can learn and improve.

The directors meet once a month to review financial results and discuss possibilities to improve the organization. Besides that, they are also actively involved in all internal and external audits performed to review and improve the Information Security Management System and corporate plans.

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

- Each year, a risk analysis is performed on the basis of the experiences of the past year and developments within the environment;
- Based on the risk analysis, improvement plans are drawn up and submitted to the board for approval;
- 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.

Controls & monitoring

Controls & monitoring are implemented through the following processes:

1. Asset & change management (incl. key management - Encryption);
2. Patch management & Hardening;
3. Capacity management;
4. Access management;
5. Incident management;
6. Third party management;
7. Personnel management;
8. Compliance management;
9. Continuity management;
10. Customer management.

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 by the board. 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 by the board.

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:

    a. A limited number of employees have access to the production environment. This only if necessary for the performance of their own work.

    b. Employees with access are given a separate user name and password, installed certificate and a second factor (time-based token) to log into the production environment. Login is via a VPN connection, which is only possible from the IP range of the Otherside office or a backup location.

    c. Access to the servers for authorised employees is restricted depending on function. Only the servers necessary for their own work are accessible.

    d. Access rights are actively updated in the event of job changes and leavers. The accuracy of the rights assigned is checked annually by the board.

    e. 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.

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 IP filtering and 2-factor authentication. Furthermore, access is only possible from the IP range of the Otherside office or from a backup location.

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 VPN 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.

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 certification audit;
3. During the annual ISAE3402 type II 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 periodic awareness sessions and, if caused by an individual or department, with the employees involved. 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 employees of Otherside at Work perform 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 at Work may retain the certificate.
- Once per year, an ISAE3402 type II audit performed by an external certified auditor. The auditor issues a signed declaration of the checks performed and the consequences for customers.

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 currently performed by Deloitte.

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

Backup & restore procedures

Data is protected against destruction by a backup process which is performed on customer databases on the past 7 days, 3 weeks (before that for 7 days) and 11 months (before that for 2 weeks) basis (thus effectively for a maximum of the last 12 months). The backups are encrypted and periodically checked by means of restores. Because there are separate backups per customer, restores per customer are possible. Thanks in part to this, Otherside can guarantee that, if desired, all the data of a specific customer can be destroyed.

Otherside has set up a permanent backup location. If the primary location is destroyed, the application can be brought back up and running within the period agreed in the SLA.

A.4 Risk Assessment

Otherside at Work (as part of its ISO 27001 certified ISMS) conducts an annual risk assessment with its daily management team. The process considers both internal and external risk factors and all assets present within the organization. Risk factors are maintained by the security officer (based on market standards) so that all relevant items are included in the assessment. These include 'Act of God'-events, insider-actions, outsider-actions, HR-problems, quality problems, growth problems, environment changes.

Risks are evaluated in a uniform manner by all departments (management team has input from all departments in the organization). Improvement plans are made based on this risk assessment and they are included in the annual audit plan. Therefor also external auditors will review the completeness of the risk assessment.

The board of Directors approves the conducted risk assessments.

A.5 Information & Communication

Within Otherside at Work various methods of communication to assist employees with understanding their individual roles and corporate controls have been implemented. New employees receive an individual introductory course in which procedures and responsibilities are explained. These include stipulation that timely communication of significant events is necessary and to which person they must report if they suspect such an event. On top of that, twice a year, sessions are held for all employees to discuss the latest development in security procedures, practices and tools within Otherside at Work as well as external development of regulatory requirements and technology. Impact on Otherside at Work is discussed.

In case of important developments identified by weekly security-meetings these are also communicated to all employees within the organisation.

Employees receive written employee-manuals which describe roles and responsibilities. These include explanations why certain tasks require two employees to be completed. All Employees also sign confidentiality agreements.

The Security Officer communicates with the relevant process managers when needed. Every month the security officer meets with the MT to discuss important learnings of incidents as well as progress in the improvement plans for the year.

A.6 Monitoring

The information security officer oversees risk assessment and monitoring activities for Otherside at Work and reports directly to the board of directors. Yearly updated risk assessments and management-team feedback are used to determine necessary resources and audit-activities. Contacts are selected which oversee these audits and suggest improvements.

To make sure audits are done correctly, auditors and auditees are stimulated to suggest improvements during their audits. Also external reviews of these audits are performed. For the secure development process an ethical hacker is selected (and changed every few years). For the management system external reviews are part of the ISO 27001 certification.

Improvements identified during the internal or external audits followed up by the contacts that are responsible for the selected business process. The follow-up activities are monitored by the information security officer and discussed in the weekly security-meetings.

All in the Statement of Applicability mentioned ISO 27001:2013 annex A controls, as well as the ISMS itself, and previously identified defects/improvements are audited.

Results are also shared with and discussed by Otherside at Work Directors. Follow up is approved by the board of Directors.

A.7 Business Processes

The business processes that are part of this statement, include:

1. System development process
2. Hosting & monitoring (OTAP patch mgt, OTAP asset/change mgt, capacity mgt)
3. Support and maintenance
4. Incident management
5. IT office management (access mgt, office patch mgt, office asset/change mgt)
6. Supplier management
7. Personnel management
8. Compliance management
9. Continuity management

Otherside at Work also services the implementation of software at clients. This is, however, not part of this SOC II type II statement, because the results of this process are easily monitored by the customer himself.

These processes are described in detail in the following paragraphs.

A.7.1 System development

Otherside at Work follows multiple guidelines to ensure its software development is secure. Ate the design phase security is included as a requirement. Also, with every individual change the impact on security is described and reviewed by a second developer. A checklist is available for the reviews, which include input from the OWASP-top 10 guidelines, ISO 27002 controls and the NCSC en NIST guidelines. All these guidelines are translated to specific guidelines applicable in Otherside at Work's development environment.

With every release of a new version of the software this new version is also reviewed and the checklist delivered to maintenance& support (which accepts new versions of the software after completing its own tests.

At least once a year an external party also performs penetration-tests on our software. The external party is regularly changed.

Competences of developers are being actively challenged and training on secure programming is done also at least once a year.

A.7.2 Hosting & monitoring

The production hosting environment is physically and virtually completely separated from Otherside at Work's office and development/testing environment. Employees are specifically granted access on a need to know and need to have basis. Employees with access can no longer access the production environment when they are no longer working for Otherside at Work, or no longer need access due to changed roles within Otherside at Work. Employees with access are actively reviewed by Otherside at Work's Directors on a yearly basis.

Access is obtained with 2FA and an IP filter so that only from Otherside at Work offices or a backup location a VPN connection with the production environment can be established.

New versions of the software, or other procedures that need to alter customer data are always first deployed on an acceptance-environment and tested and accepted by maintenance & support before being deployed and executed on the production data.

The virtual OTAP-environment is managed by a source-code tool as well (infrastructure-as-code) so (virtual) servers are easily restored to a previous version if problems arise. Also: all change are through the source code. Manual access to (most of) the servers is not configured.

Customer data is protected through 7 day, 3 week and 6 month-backups of all individual customer databases. These are stored encrypted on a physically different location.

Backups are regularly (at least once a month) tested by doing a restoretest. Because all customers have separate databases, Otherside at Work can guarantee active destruction of data in all backups if individual customers should request so.

Backups can only be removed with the help of one of the managers of Otherside at Work and another employee. No single employee can remove backups of customer data. A permanent disaster recovery environment is present to make sure production can be up-and-running again within 24 hours.

To monitor production both a monitoring and SIEM application are used. The SIEM can actively escalate when certain patterns in the logs are identified.

Patch management is actively performed (when necessary due to security risks within 1 week after a patch is released). Vulnerability scanners are in place.

The firewall only allows actively set traffic. All web traffic is SSL/TLS encrypted. File transfer is done over VPN or SFTP.

The network of the production environment is also segmented, so database servers aren't reachable over the internet.

Data at rest is stored encrypted (TDE on SQL Server and disk encryption for received files). Also cell-level encryption for medical data is in place.

Uptime is measure from outside of the network and actively monitored through 24/7 monitoring (Pagerduty). Resource consumption is also actively monitored with acceptable threshholds to detect a bottleneck before it's an issue.

A.7.3 Support and maintenance

Customer application administrators can create roles and users themselves. Otherside at Work only authorises the first administrators. Administrators can use several reports to make sure roles and authorization are set correctly.

Support monitors uptime of all applications. It also monitors and counts received calls per customer with response times, to monitor if agreements in SLA's with customers are being met.

Support & maintenance also accepts new versions of the Otherside at Work software after performing structured tests, based on impact analyses of changes included in the new version. Parts of these tests are automated. Every release more automated tests are included, based on previous incidents and changes.

A.7.4 Incident management

Incidents can be reported by customers or Otherside at Work employees, or they can be found when audits are performed on controls by responsible contacts within Otherside at Work.

When an incident is reported and confirmed, an improvement plan is made. These may include the introduction of additional controls. It is actively checked whether existing procedures are sufficient to prevent recurrence of the incident. An incident-database is maintained for future evaluation and a necessary casefile.

Security incidents are always reported to the security officer and customers involved. At the latest within 24 hours, so customers can fulfil their responsibilities to the 'Autoriteit Persoonsgegevens'.

A.7.5 IT office management

IT office management has a separate management process (and department) from the OTAP-environment where Xpert Suite is hosted. 'IT services' manages the internal office environment. This contains asset management, access management, backup management and patch management and hardening.

All laptops contain encrypted disks. Virtual access to the office environment is through 2FA VPN connection and only allowed on devices managed by IT Services.

Office 365 is used for e-mail and office software and document management. Data is backupped separately to provide continuity.

IT services manages security through endpoint-protection solutions (anti-malware and anti-virus) and all links in e-mails have extra measures to protect against phishing attempts.

A.7.6 Supplier management

All suppliers go through a managed procurement process. Standard analysis checklists are present to determine suitability of the provider (based on continuity and confidentiality risks). For high risk suppliers the board approves procurement (based on advice by IT services and security officer). These include necessity of ISO27001 certification when personal data is processed by suppliers.

Personal data of the users of the Xpert Suite are not processed by other parties than agreed with our customers in the data processing agreements.

Necessary controls are part of the supplier agreements and monitored through a yearly auditing process.

A.7.7 Personnel management

The HR policy has already been described in paragraph '3.4 Control Environment Elements'.

A.7.8 Compliance management

Through the compliance management process Otherside at Work monitors whether it is compliant with alle applicable laws for its services and internal processes. A special focus is on compliancy with the GDPR regulation, for which a privacy officer and DPA are appointed to help the internal organisation to change the processes to be in accordance with the GDPR. For general 'compliance management' and external advisory firm is hired to update the management team and security officer on changed laws and regulations.

A second important process is the compliance with the Xpert Suite with the laws we support our customers with (WVP, WAZO, AP guidelines, etc.). Compliance management for the Xpert Suite is managed by product management, who are in contact with the relevant institutions (UWV and AP) to update the software where necessary.

A.7.9 Continuity management

The goal of continuity management is to have a controlled method by which information security can be maintained under special circumstances.

1. Based on the annual risk analysis, the risks with low probability but very high impact are assessed.
2. In doing so, it considers:
    a. Whether the known scenarios provide adequate guidance for dealing with the occurrence of such a scenario
    b. OR whether an expansion / new playbook needs to be drafted
3. Management then periodically reviews the roadmaps for content and risk assessment (whether additional roadmaps are not required). This is included in the management review.
4. Contingency plans are assessed at least every 2 years via a (table top) simulation. This is done with the contact persons responsible for sub-areas. Improvements to the plans are also discussed directly.

A.8 Management control

Management performs the internal audits themselves. Also: all responsible contacts for the relevant security processes are members of the management team. Therefor management is always actively involved with improvements and the daily work procedures. This improves the openness as well.

A management review of the ISMS is also done yearly to determine if necessary resources and tooling are available to achieve the desired goals.

A.9 Complementary User entity controls

In designing its system, Otherside at Work has contemplated that certain complementary controls will be implemented by user organizations to achieve certain control objectives included in this report under their control or supervision:

- Customers are responsible for establishing physical security protections over all workstations, servers and communication hardware that interface with their managed hosting environment and that are housed in their facilities or other locations.
- Customers are responsible for reporting any processing problems encountered to Otherside at Work and for providing such assistance as is necessary to permit problem resolution.
- Upon notification of a maintenance window, the customer should take appropriate, timely action based on the notifications that are sent.
- The customer is responsible for controls governing access to functionality and data used by their application. This includes the use of application configuration parameters and database configuration.
- The customer is responsible for identifying upgrades/changes/patches that are to be made to the user workstations/networks/environment.
- The customer is responsible for specifying initial firewall settings, and for initiating any changes to the existing configurations as needed.
- The customer is responsible for administering logical access to the Xpert Suite portal accounts.
- The customer is responsible for administering local user and administrative accounts on their servers.
- The customer is responsible for appropriately monitoring and aiding in the resolution of change management tickets, as needed.
- The customer is responsible for obtaining, monitoring, and appropriately using SSL encryption client settings.
- The customer is responsible for requesting the initiation of the data restore process, if necessary.

A.10 Complementary Subservice Organization Controls

Otherside at work B.V. uses subservices organisation Proserve BV to provide Hosting Services. The services consist of Networking, Compute/Storage and Virtualisation. Further Proserve B.V. and Otherside at Work are jointly responsible via a so called 'vitual team' for: Virtualisation (non-root vDOM's), Virtualisation (member of the virtual team have access to VMware), Operating System, Middleware and Runtime.

The complementary controls implemented by Proserve B.V. are related to:

3402-type II (categories respond with the Annex A of the ISO 27001/2013)

- Information Security Policies.
- Organization of Security.
- Responsibility for Assests.
- Information Classification.

- Media Handling.
- Business requirements of Access Control
- User Access Management.
- System and Application Access Control.
- Secure Area's.
- Equipment.
- Operational Procedures and Responsibilities.
- Backup.
- Logging and Monitoring.
- Control of Operational Software.
- Technical Vulnerability Management.
- Network Security Management.
- Management of Information Security Incidents and Improvements.
- Information Security Continuity.
- Redundancies

ISO 27001/2013 All controls revered to with the ISAE 3402 and complimented with the controls below

- Human Resource Security
- Access Control
- Cryptography
- System Acquisition, Development and Maintenance
- Supplier relationships
- Information Security Incidents
- Compliance

3000D-type II (categories respond with the Annex A of the ISO 27001/2013)

- Access Control
- Cryptography
- Operational Security
- Communications Security
- System Acquisition, Development and Maintenance
- Compliance

To determine if Proserve provides their service within our expectations we will check their ISAE3402-type II report, ISO/IEC 27001 certification and we have assigned a third party auditor to provide us annually with a 3000D-type II assurance report for specified additional assurance on controls as – high level – specified above.

Appendix B: Service obligations & mandatory compliancy laws and regulations

B.1 Service obligations - SLA

The standard SLA of the Xpert Suite (and therefor our service obligations contain the operation of Xpert Suite, the provision and performance of support and maintenance, including the further development of Xpert Suite, and the related activities. These services are provided at the Service Level agreed upon in the SLA. The SaaS solution Xpert Suite consists of the following services:

- Operation:
  - Continuity, capacity & availability management;
    These contain the locations for processing, escrow-services and availability requirements (standard 99,6%)
- Service desk; Xpert Desk: support of Client's application management:
  - Incident management;
    These contain ways customers can contact the servicedesk and responsetimes that Otherside has to achieve.
  - Change management;
    These contain the agreed processes for change-requests.
- Version control and deployment:
  - Release management.
    This contains the process for deploying new releases (including service windows) and informing customers about the changes made. It also obligates Otherside to test that releases don't interfere with ongoing operations.

In addition to the services delivered by the Xpert Desk, Otherside can also deliver services for first line support and functional management under direction of the Client. These additional services could be agreed by signing an addendum called Functional Application Management. A fixed capacity per month is assigned to the Client and is carried out by professionals from Otherside who have been trained for this purpose and who have the skills to carry out the tasks described in the addendum. First line support and functional management are not subject to the SLA.

B.2 Laws & Regulations

The Xpert Suite is used for processing personal data of EU citizens. Primary obligations therefor arise from the GDPR and the derived regulations issued by the 'Autoriteit Persoonsgegevens' in The Netherlands or other authorities dependent on the location of the customers (which are the controllers for this personal data).

Otherside is only the controller for their internal processes (HR, sales, etc) and is subject to the Dutch AP for these processes.

With the Xpert Suite we also support our customers to act in accordance with the local working condition laws (i.e. 'Arbeidsomstandighedenwet' in the Netherlands) and derived other laws around 'work related social security (i.e. the WIA and ZW in the Netherlands).