otherside at work
for happy professionals

SERVICE LEVEL AGREEMENT
XPERT SUITE

AUTHOR Rob Brekelmans

FUNCTION Manager Operations

VERSION 5.0

STATUS Final

DATE 10 June 2020

CLASSIFICATION Sensitive

powered by
fair priced technology

TABLE OF CONTENTS

GENERAL

1.1 LEGAL LINK WITH AGREEMENT & CHANGE MANAGEMENT SLA

Client and Otherside have entered into an Agreement for the service and its provision. The Agreement is guiding between the Parties involved and this Service Level Agreement (SLA) is an elaboration of the support and maintenance element within the framework of the Xpert Suite Software and Services that are offered as a Software as a Service (SaaS) solution.

The commencement date of the SLA is the go-live date of the software. The obligations in this SLA cease to apply when the Agreement between Client and Otherside is terminated.

1.2 SCOPE OF THE SERVICES

Parties aim for a long-term relationship regarding the development of occupational health & absenteeism processes using the SaaS solution Xpert Suite. The services agreed in connection with that relationship concern the operation of Xpert Suite, the provision and performance of support and maintenance, including the further development of Xpert Suite, and the related activities as set out in the Agreement and this SLA. These services are provided at the Service Level agreed upon in this SLA. The SaaS solution Xpert Suite consists of the following services:

- Operation:
  - Continuity, capacity & availability management;
- Service desk; Xpert Desk: support of Client's application management:
  - Incident management;
  - Change management;
- Strategic release development:
- Version control and deployment:
  - Release management.

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.

1.3 SERVICE DESK; XPERT DESK

The functional application manager of the Client carries out first-line service desk activities for the Client's users. Only the functional application managers and selected key users of the Client (Super Users in Xpert Suite) can present functional and technical questions about the operation of Xpert Suite to the service desk of Otherside; Xpert Desk. Questions and faults will be dealt with in accordance with the response and resolution times laid down in this SLA. The Xpert Desk of Otherside can be reached during the opening hours specified in the SLA. The Client does not have to pay any extra costs for consulting Otherside's Xpert Desk (this is included in the software rate), unless stated otherwise.

The Xpert Desk of Otherside registers, monitors and reports on the handling of incidents and changes. As of the commencement date of the agreement, Otherside will give the "Xpert Suite Super Users" of the Client access to the service management application of Otherside, so that the authorised officers of the Client can register the incidents and

changes there directly, following which Otherside will process and monitor the incidents and changes in accordance with the agreed Service Levels.

1.3.1 ACCESSIBILITY

Functional Questions, Service Questions (e.g. request for repair actions, database copy requests, etc.), , Product Suggestions, Bugs and Malfunctions can be submitted:

- via the service management application of Otherside (recommended for incidents with priority 3 and 2 and changes):

As Super User access via Xpert Suite application	

- by email:

24 hours / 7 days a week	xpertdesk@othersideatwork.nl

- by telephone (recommended for tickets with priority 1):

During office hours Monday to Friday 8.30 - 17.30h	+31 73 6159999

- by priority email (only for tickets with priority 1), on call engineer will react within an hour:

Outside office hours and public holidays	storingen@othersideatwork.freshdesk.com

1.4 DATA & SECURITY

1.4.1 SECURITY OF INFORMATION

Otherside attaches great importance to the security of data for its Clients. The high standards we set for this are reflected in physical, technical and procedural measures that we impose (both internally and with respect to our suppliers), adhere to and monitor.

Otherside's security approach involves:

1 Embedding information security in the organisation;

2 Logical and physical access security;

3 Functional management, connections and hosting;

4 Monitoring and improvement of security measures & security incidents;

5 Software development;

6 Backup & restore procedures.

Otherside has an ISO 27001:2013 certificate and can also produce an ISAE 3402 Type II declaration. 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.

Information security is managed via the ISO 27001 certified Information Security Management System (ISMS), registered via the BSI Group under certificate number ISC-077. It is managed by the 'security officer' who is also a member of the management board. 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 management team for approval;
- After approval, the implementation of these points for improvement is monitored fully by the MT in the running of the company.

As well as the management system itself, management processes are set up for which responsibilities are separated. For each process someone has final responsibility who, in consultation with the management board, determines when and which controls take place. Whether or not each person responsible actually tackles their 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 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 Client management.

Within personnel management, attention is expressly paid to:

- Awareness about information security; knowledge evenings are held several times per year examining the importance of information security for our clients 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 employee handbook 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 clients about whom information is recorded in our systems. The aim here is not only to motivate employees to follow the procedures exactly, but also always to keep thinking critically about whether actions are being performed that could have serious negative consequences for our Client(s) and thus also for Otherside itself.

- Competencies; When someone joins the company and each year thereafter, an active assessment is made of whether the competencies of the employee concerned 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) requested;
  - Signing of a declaration of confidentiality;
  - Client-specific screenings.

- Active assessment of adherence to 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 security incident caused personally is assessed much less negatively than if another employee reports it. This is to prevent a culture of fear from developing.

1.4.2 LOGICAL AND PHYSICAL ACCESS SECURITY

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

1. No employee of Otherside has independent physical access to the areas where client data is stored. This always requires the cooperation of the hosting partner (Proserve) and the approval of the management board;
2. Proserve employees can physically access the equipment on which client data is stored. However, this data is stored on encrypted disks and in encrypted databases, making the client 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 management board. The areas covered in this key plan are: workstations (general), workstation financial administration, server room office environment (no client 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 management board;
5. The joining and leaving protocol includes a check list used to verify that all physical and logical access is closed. In addition, the check list 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 is granted only if necessary for the performance of their own work;
   b. Employees with access are given a separate user name and password, an installed certificate and a second factor (time-based token) to log into the production environment. Login takes place 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 position. Only the servers necessary for their own work are accessible;
   d. Access rights are actively updated in the event of job changes and when leaving the company. The accuracy of the rights assigned is checked annually by the management board;

e Just as for all other users, access to production databases via the web interface is always secured with 2-factor authentication;

f Web traffic is always secured via SSL and the SSL settings are tested for known vulnerabilities using external tools. File exchanges take place via Webservices or SFTP.

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.

1.4.3 MANAGEMENT, CONNECTIONS AND INFRASTRUCTURE

Within the Xpert Suite, the client administrators themselves can define and assign roles to users. Based on these roles, the software determines which changes users may or 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).

Otherside takes care of the management of the medical files in the Xpert Suite for employers on the instructions of the hired occupational health and safety service / company doctor. Functional management includes all management activities related to medical files, like adding new documents, adding users, adding or modifying authorisations, but always on the instructions of the occupational health and safety service / company doctor in connection with the guidelines of the General Data Protection Regulation (GDPR).

For the management of the servers that the software and client data are stored on, an employee of Otherside 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 an 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 is allowed that has been explicitly opened and thus approved via the change procedures. The traffic is then routed over a segmented network whereby only the web and connection servers that are intended for this are accessible via the Internet.

Web traffic is always secured via SSL and the SSL 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 Client. 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 client and application key.

1.4.4 MONITORING AND IMPROVEMENT OF SECURITY MEASURES AND SECURITY 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 As a result of the analysis of a reported security incident.

Security incidents can be reported by Client(s) or employees or can be the result of a (periodic) check of a management 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 which 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, it is expressly determined for each measure in what way and how often its effectiveness is measured. 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 regular awareness sessions and, if caused by an individual or department, with the employees involved. If a security incident leads to a (potential) data breach, the 'Duty to Report Data Breaches' procedure is followed. As part of this procedure, data controllers must be informed within 24 hours in accordance with the guidelines of the Dutch Data Protection Authority.

1.4.5 SOFTWARE DEVELOPMENT AND INFORMATION SECURITY

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 check list for this, which is based on the OWASP top 10 guidelines, ISO27002 controls, NCSC and NIST. For each release, the modified code is reviewed against this check list and delivered to the Xpert Desk. The Xpert Desk 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 years to ensure a critical analysis. These are always reputable parties such as (but not limited to) Deloitte, Dionach and Fox IT.

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

1.4.6 BACKUP & RESTORE PROCEDURES

Otherside undertakes to have the Xpert Suite optimally available. For this purpose, Otherside makes daily backups of the application, database and log files on a remote server while keeping a fall-back location available. Changes as regards Xpert Suite will also be recorded continuously in log files. By default, a history of seven days maximum is used. If agreed in the contract, the history covers a longer period.

Data is protected against destruction by means of a backup process that was performed on client databases over the past 7 days, 4 weeks and 6 months. The backups are encrypted and regularly checked by means of restores.

Otherside has set up a permanent backup location. Should the primary location be destroyed, the application can be brought back up and running within 24 hours.

Because there are separate backups per Client, restores per Client are possible. Also because of this, Otherside can guarantee that, if desired, all the data of a specific Client on the production environment can be deleted. Partial deletion of data in the backup environment isn't possible. The backups will automatically be destroyed within 6 months.

The Client can make a request for a Restore action via the Xpert Desk. If the Restore is a result of incorrect or incompetent use of Xpert Suite, the costs will be charged. In the event of calamities, the Client may choose to continue working with a back-up version of the database. The backup is placed on a different server, so as to limit loss of data in the event of a calamity as much as possible. The costs based on applicable tariffs (ask for the actual tariffs upfront) for these restores will be charged.

The process for this request is as follows:

- Client requests the restore by telephone at the Xpert Desk. A Service Request ticket will be created;
- This request states the reference date of the backup on which the restore must be delivered;
- The Delivery Manager of Otherside confirms receipt of the request, the costs and the execution in accordance with the request. Based on mutual discussion, this written confirmation will state when the restore will be executed (normally within two workdays);
- The restore is checked by the Client and, if approved, a written discharge by the contact person of Client is given to the Delivery Manager of Otherside.

1.4.7 RETENTION PERIODS AND DESTRUCTION

Otherside facilitates the Client in meeting the retention periods and the timely destruction of data. Otherside will never independently destroy data without an underlying express instruction from the Client, or where the termination procedure from the General Terms and Conditions has been followed. Partial deletion of data in the backup environment isn't possible. After destruction of data on the production environment, the data is only available in the backups for 6 months.

1.5 EXIT PROCEDURE

If the agreement between Otherside and the Client is terminated in the usual manner and if the Client has fulfilled all its obligations towards Otherside, Otherside will place the data once-only in a backup file for an MS SQL server database, which can be read back into the Client's MS SQL server. This is done free of charge.

It is also possible for the Client to receive an export in Excel or RTF formats. The following data is supplied in Excel format:

- Organizational data;
- Employee data;
- Absence history;
- Form fields (data entered in screens);
- Tasks, notes, instructions and contact moments (running, executed).

The documents from the Xpert Suite are delivered in RTF, split into medical and non-medical. The uploaded documents are delivered in the format as uploaded. The costs (based on 2020 rates, ask for the actual rates upfront) for these exports are per export:

- € 861 excl. VAT for the document export;

- € 574 excl. VAT for the Excel export.

The process for this request is as follows:

- Client requests the data in writing or by email from the Client's Delivery Manager of Otherside. This request states the reference date on which the data must be delivered and whether multiple deliveries (e.g. 1 trial delivery on date X and 1 final delivery on date Y) or one delivery must take place;
- The Delivery Manager of Otherside confirms receipt of the request and the execution in accordance with the request and the associated conditions as included in this exit plan. Based on mutual discussion, this written confirmation will state how the data will be delivered and to which authorised person (by SFTP, by secure DVD, etc.);
- The data are delivered to the Client's contact person on the agreed date and by means of the stated method;
- The data are checked by the Client and, if approved, a written discharge by the contact person of Client is given to the Delivery Manager of Otherside;
- Otherside will store and keep available all Client files and data up to 60 days after the agreement has been terminated by giving notice of termination or as a result of annulment so that the Client (or the third party designated by the Client) can retrieve or destroy its files and data. After expiry of that period, Otherside will delete the files and data unless the Client requests Otherside in Writing to keep the files and data for an additional period to be determined at such time in more detail by the Client. Partial deletion of data in the backup environment isn't possible. After destruction of data on the production environment, the data is only available in the backups for 6 months.

1.6 CONSULTATION STRUCTURE AND SLA REPORTING

Client will on its request receive the service report from Otherside over the past calendar quarter. The SLA report describes as a minimum:

- An overview of the number of registered tickets in the past quarter by type of incident:
  - Functional Questions;
  - Bugs;
  - Malfunctions;
- An overview of the number of registered tickets in the past quarter by type of change:
  - Service Requests;
  - Product Suggestions;
- An overview of the number of closed tickets per type of incident with a maximum historical period of 6 months;
- An overview of the number of tickets by status:
  - That are being handled by Otherside;
  - That are being parked outside Otherside;
- An overview of the incidents in the past quarter;
  - Which % of the Bugs were fixed on time and which % were not fixed on time;
  - Which % of the Malfunctions have been responded to timely and which % have not been responded to timely;
  - Which % of the Malfunctions were resolved in time and which % were not resolved in time;
- The availability for the Xpert Suite in the past quarter.

If the agreed Service Level is not met, or if there are other points of attention in the provided service, the following escalation model applies:

ESCALATION LEVEL	CONTACT PERSON CLIENT	CONTACT PERSON OTHERSIDE
LEVEL 1	Functional application manager	Employee Xpert Desk
LEVEL 2	Coordinator functional application management / service level manager / IT manager	Delivery Manager
LEVEL 3	Contract owner	Account Manager
LEVEL 4	Management board	Manager Operations

By default, Otherside suggests the following consultation structure:

2 x per annum:	Service Level Consultation (account manager, delivery manager, Client)
1 x per quarter:	Business Account consultation (account manager, Client)
1 x per annum:	Strategic consultation (management board and account manager, Client)

A definitive consultation structure will be set up in consultation with the Client.

2 CONTINUITY, CAPACITY & AVAILABILITY MANAGEMENT

2.1 HOSTING

The Xpert Suite is hosted in a physical certified data centre of Dataplace in Alblasserdam (www.dataplace.eu). For redundancy backups are also stored in a separate physical data centre of EUNetworks in Amsterdam (www.eunetworks.com). Otherside guarantees a 99.6% availability of the Xpert Suite and that all data is processed within the EU/EEA. The hosting also includes:

- Making the application available and access to the database on an internet server;
- Security of the data in the database (backup and firewall protection);
- Management and maintenance of hardware and software;
- The management and maintenance of Xpert Suite (keeping the functionality up to date, particularly as regards laws and regulations relating to absence).

2.2 CONTINUITY AND ESCROW

Otherside realizes that under certain circumstances - and solely for the purpose of ensuring the continuity of the Software - the Client may wish to have the source code of the Software at its disposal. In this context, Otherside has deposited the source code of the Software with a specialised escrow agency. This deposit is renewed as soon as there are any significant changes to the Software. The agreement with the escrow agency includes a third-party clause for the benefit of the Client, which provides, put briefly, that the escrow agency may issue the source code to the Client in the event of discontinuity of the Software, subject to further conditions. The Client can join the escrow agreement concerned as a beneficiary.

Subject to the condition that the source code has been issued in accordance with the agreement between Otherside and the escrow agency, Otherside grants the Client a right to use the Software for its own use and to adapt the Software for the purpose of maintenance and further development. This conditional right of use shall under no circumstances include the right to exploit the Software other than for its own use and that of its end users.

Client can register as an Escrow beneficiary. A registration form has been added to the annex to this SLA.

2.3 AVAILABILITY

Otherside guarantees the following availability for the Xpert Suite:

AVAILABILITY[1]
99.6%

1 Otherside will make the delivered Xpert Suite service as described in the Agreement available for seven times twenty-four hours (7*24) per week;

2 Otherside guarantees an availability of 99.6% with respect to the delivered SaaS solution Xpert Suite as described in more detail in the Agreement. The above-mentioned availability is measured and calculated over the period of

[1] This concerns the availability of the entire SaaS solution Xpert Suite.

one (1) calendar quarter. Otherside undertakes to comply with the service level chosen by the Client as described in this SLA;

3 Up to the Public Internet, Otherside guarantees an availability of 99.6% 7*24 hours on a quarterly basis. Otherside does not guarantee that communications via the internet are always possible, that a connection can be made at all times with another machine that is connected to the internet, or that the service Xpert Suite can always be accessed via the internet. The demarcation point is the outermost point on Otherside's firewall with the public Internet. If there's a problem on Otherside's side of the demarcation point, it's Otherside's responsibility to solve it;

4 The availability guarantee takes effect the moment that the Xpert Suite service has been delivered to the Client in operational state;

5 The Client must report any Malfunctions concerning the Xpert Suite service as soon as possible by telephone or electronic means to the Xpert Desk;

6 The period of "unavailability" commences at the moment that the Client reports and/or Otherside discovers that the Xpert Suite service no longer functions in accordance with the specifications agreed between the parties as stated in this SLA;

7 The period of "unavailability" ends the moment that Otherside notifies the Client that the Xpert Suite service is functioning again in accordance with the specifications agreed between the parties as stated in this SLA;

8 The Availability (A) is calculated as follows:

a A: ((Nt - Dt)/Nt) x 100%;

b Nt: Time period during which the Equipment and/or Software must be available;

c Dt: Time period that the service is not available (time during regular Maintenance Window excluded).

During the Maintenance Window, the availability guarantee does not apply. Availability is measured over the period of one full calendar quarter. The availability of the service and access security is monitored 24 hours a day, 7 days a week.

3 INCIDENT MANAGEMENT

With incident management we mean the treatment of support questions and solving disruptions. The purpose of incident management is to restore normal services as soon as possible to minimize the consequences by explaining the working of a specific functionality or investigation and solving a fault.

3.1 TYPE OF INCIDENTS

We distinguish three types of incidents:

- Functional Question;
- Bug;
- Malfunction.

3.2 FUNCTIONAL QUESTION

As stated before, the functional application manager of the Client carries out first-line service desk activities for the Client's users. Functional and technical questions about the functioning of the Xpert Suite, for which the functional application manager(s) and first line support for the Client do not know a solution or for which the Client cannot realize the solution independently, can be raised without limitations by the (functional application manager(s) and key users of the) Client with the Second Line Support team part of Otherside's Xpert Desk department.

Support is subject to a fair usage policy. If lack of experience by the functional application manager is the reason of relatively much support, the Delivery Manager will establish contact with the Client to discuss the service to be delivered and to draw a statement of work or new addendum.

3.3 BUG AND MALFUNCTION

When it is reported that the Xpert Suite does not function as reasonably can be expected (final judgement by Otherside) and the reported problem can only be solved by modifying this application, this is called a Bug. When the reported problem is caused by misfunctioning of the platform and therefor can only be solved by modifying the infrastructure, this is called a Malfunction.

3.4 PRIORITIZATION INCIDENTS

After a Functional Question, Bug or a Malfunction is approved, the priority will be determined. We distinguish three classifications of approved incidents:

- **Low impact**: the incident has very little impact on working with Xpert Suite, e.g. a workaround is available. The incident doesn't result in data inconsistency and data integrity, security and privacy are covered. Working on a fix is low prioritised;
- **Medium impact**: the Incident can be fixed by a small modification in the application or the platform. To fix a Bug or Malfunction, usually no functional and/or technical design is made. However, the existing documentation is brought in line with the changes in the SaaS solution Xpert Suite and a brief description is given in the service management application of how the Bug or Malfunction was fixed. High priority fixes are usually taken into production with an intermediate update (hot fix) at night or during the weekend. Other fixes will be part of a regular release and update during a Maintenance window;

- **High impact:** that the incident can only be solved by modifying the Xpert Suite application. In this case, however, the modifications are so extensive that a formal process must be completed, consisting of the following steps: requirements analysis, drawing up functional and technical specifications, building, testing and putting into production.

Urgency is associated with time. The time it takes to have the perceived Impact:

- Low urgency:
    - The damage caused by the incident only marginally increases over time;
    - Work that cannot be completed by staff is not time sensitive;
- Medium urgency:
    - The damage caused by the incident increases considerably over time;
    - A single user with VIP status is affected;
- High urgency:
    - The damage caused by the incident increases rapidly;
    - Work that cannot be completed by staff is highly time sensitive;
    - A minor incident can be prevented from becoming a major incident by acting immediately;
    - Several users with VIP status are affected.

Incidents are dealt with on the basis of priority by using the priority matrix:

		URGENCY		
		Low	Medium	High
IMPACT	Low	Priority 3	Priority 3	Priority 2
	Medium	Priority 3	Priority 2	Priority 1
	High	Priority 2	Priority 1	Priority 1

This led to three types of priority that can be distinguished:

1. Priority 3:
    i Low impact Bugs and Malfunctions: Business functions are possible, but the error situation is perceived as annoying by the user;
    ii All Functional Questions;
2. Priority 2:
    i Medium impact Bugs and Malfunctions: Non business-critical functions are blocked;

3. **Priority 1**:

   i High impact Bugs and Malfunctions: Business-critical functions are blocked. A workaround solution may be desirable / necessary.

The priority is determined by the Client after which Otherside tests it. In case of different opinions, this will be solved via the established escalation lines.

Otherside checks whether the ticket:

- Has been placed in the correct type of incident (Functional Question, Bug or Malfunction) ;
- Has been assigned the correct priority (1, 2 or 3).

If the type of incident and/or prioritization is incorrect according to Otherside, feedback will be provided to the Client. Escalation takes place in accordance with the escalation model.

3.4.1 SPECIAL INCIDENTS: SECURITY

In addition, Otherside distinguishes security incidents as a special category. These are assessed on the basis of a risk analysis (how much data, what type of data, risk of abuse). If there are major consequences for clients, stakeholders or Otherside, immediate action is taken to resolve the security incident. One of the options that can be chosen is to make wider data inaccessible to users, so that any data breach is also stopped. In every other respect, the procedures described in section 1.4 apply.

3.5 SERVICE LEVELS INCIDENTS

The following service levels apply to the handling of incidents by the Xpert Desk. First line support and functional management are not subject to these service levels.

	DESCRIPTION	RESPONSE TIME	RESOLUTION TIME [1]
PRIORITY 3	Bugs and Malfunctions: Business functions are possible, but the error situation is perceived as annoying by the user Functional Questions	75% within 8 hours	75% in accordance with planning (if a resolution is jointly agreed) [2]
PRIORITY 2	Bugs and Malfunctions: Non business-critical functions are blocked	90% within 4 hours	75% within 1 working week
PRIORITY 1	Bugs and Malfunctions: Business-critical functions are blocked. A workaround solution may be desirable / necessary. Security Incidents	99% within 30 minutes [3]	75% within 1 working day

[1] Outside office hours and on public holidays, only priority 1 incidents are handled. Priority 3 and 2 are handled as from the next working day, in accordance with the above service levels.
[2] This concerns the planning as agreed with the Client and assigned to a release.
[3] The response time for priority 1 incidents can only be guaranteed if the report is made by telephone or priority email (see 1.3.1).

4 CHANGE MANAGEMENT

4.1 TYPE OF CHANGES

We distinguish two types of changes:

- Service Request;
- Product Suggestion.

4.2 SERVICE REQUEST

For remote or online support not covered by the types of incidents, a ticket is classified as Service Request. This includes outsourcing of or support:

- (Re)configuration;
- (Re)implementations of functionalities and processes;
- Imports and exports of data;
- Repair actions;
- Data modifications: making corrections in the Xpert Suite database that the Client's first-line support cannot make itself via the application (e.g. correction of a period of illness);
- Training of Xpert Suite users and functional application managers;
- Making a copy of the database (e.g. for training purposes).

Remark: In connection with the GDPR, Otherside only makes corrections to the Xpert Suite database after Otherside has received express consent from the (client of) the Client.

The Account Manager or Delivery Manager will take care of such a request and will establish contact with the Client to discuss the service to be delivered and to draw a statement of work. Otherside may charge a fee for the handling of Service Requests. Otherside will indicate in advance when a fee will be charged, linked to the Service Request concerned. Otherside will only start the execution after the Client has given its approval.

4.3 PRODUCT SUGGESTION

The Xpert Suite is continuously improved and expanded with new functionalities. Otherside carefully listens to its customers and users. They can influence the priorities on the product development roadmap by giving Otherside feedback and sharing ideas for functional changes or additions to the Xpert Suite. These ideas are referred to as Product Suggestions.

Product Suggestions can be submitted to the Xpert Desk and will be assessed by Otherside's product management team whether this Product Suggestion fits the product strategy of Otherside and the needs of its customers. In general only Product Suggestions of a generic nature (of interest to multiple Clients) will be adopted as part of the product development roadmap. In all cases changes will be made available to all customers unless agreed upon explicitly otherwise.

If Otherside adopts the Product Suggestion the functional change will be incorporated in the product roadmap. When the corresponding functional change has been realized, it will be released as part of a scheduled release and included in the corresponding releasenote. Separately the Client will also be informed by the Xpert Desk.

In case the Client would like to increase the priority of their Product Suggestion, Otherside can be asked to provide a quotation for the corresponding change. Otherside will submit an offer to the Client for the realization of the specific extension to the Xpert Suite. After the Client has accepted the offer, Otherside will plan and execute the change. These changes, too, are subject to the provisions set out in this SLA.

In many cases Otherside aims for co-creation with the Client in the realisation of generic Product Suggestions. This means that Otherside cooperates closely with the Client in terms of drawing up the requirements and realising the software, but it also regularly seeks financial cooperation, which makes it attractive for both parties. This way of working enables for a faster realisation of the goals of the strategic product development roadmap of the Xpert Suite and customer driven product enhancements.

4.4 SERVICE LEVELS CHANGES

Response time to Client within 4 weeks. Resolution time in accordance with planning (if a resolution is jointly agreed).

5 RELEASE MANAGEMENT

5.1 VERSION CONTROL AND DEPLOYMENT

Prior to the installation of new releases, Otherside will hand over the release notes of the upcoming release to the known functional application managers. At the Client's request, Otherside installs the new version of Xpert Suite (Beta release) in the test/acceptance environment for the Client not later than 5 working days before the release date. On the indicated release date, Otherside installs the new software version (release or update) in the production environment. Installation of the new releases/updates from the acceptance environment to the production environment takes place via an automated procedure (script). Then the Client has up to 3 working days before the release date to object with reasons against a release being put into production. In that case, the Client and Otherside will discuss whether the release for the Client or for all Client(s) should be postponed or whether the Client still participates in the release. Otherside guarantees here at least the following:

- Data exchanges with HR systems and/or other systems linked to the Xpert Suite remain intact with respect to processing on the side of the Xpert Suite;
- Any specific Product Improvement and the Xpert Suite layout will continue to function unchanged;
- There are no compatibility problems with data and information already entered in the Xpert Suite;
- By default all data in the test/acceptance environment will be anonymized by an automated procedure (script);
- Client can ask for a new test/acceptance environment free of charge once per calendar quarter;
- If Client did not use the test/acceptance environment for 6 months, by default this test/acceptance environment will be deleted. At Client's request the creation of a new test/acceptance environment will be planned.

5.2 MAINTENANCE WINDOW

The availability of Xpert Suite (production environment) can be interrupted for a short period of time for the maintenance of the servers and other hardware and for installing releases. Maintenance is carried out during off-peak periods (weekends) to disrupt availability as little as possible. If the service is interrupted for a longer period due to unforeseen circumstances, all in-service partners and the functional application managers of the Client(s) of Otherside will be informed.

ACTIVITY	PLANNED	TIME (GMT +1)
Bug fixes[1]	Daily (if applicable)	20.00h - 21.00h
Releases and updates (Slow Track)	On Thursday (once each 9 weeks)	20.00h – 21.00h
Releases and updates (Fast Track)	On Wednesday (once each 2 weeks)	20.00h – 21.00h
Releases and updates	On Saturday (once each month)	Saturday 20.00h – Sunday 02.00h
Occasional infrastructural updates	During weekends (maximum four times a year)	Friday 20.00h – Monday 04.00h

[1] Exceptionally, urgent work may also be carried out during office hours. Otherside will inform the Client of this as soon as possible in writing or by telephone.

5.3 STRATEGIC RELEASE DEVELOPMENT & FUNCTIONAL MAINTENANCE

Otherside follows its own strategic product development agenda. Based on the strategic dialogue with its Clients, perceived market developments and new technological enablers the strategic product development roadmap is composed and continuously maintained. The Client can participate as a member of the 'UserGroup' user platform. Through this platform, adjustments and innovations in the Xpert Suite are tested for feasibility and functionality, among other things. The sessions are informative, evaluative and, of course, interactive. UserGroup sessions are exclusively for the Clients of Otherside and can be attended free of charge.

Functional maintenance involves making a functional change or addition to the Xpert Suite and takes place at the initiative of Otherside or at the request of the Client. At the initiative of Otherside the necessary functional changes to facilitate new, or alterations to, relevant laws and regulations (e.g. compliance with the Dutch Eligibility for Permanent Incapacity Benefit (Restrictions) Act) are included in the product development roadmap.

6 PENALTIES

6.1 AVAILABILITY

If the Services do not achieve Availability in accordance with clause 2.3 of this SLA, Client has the right to claim a penalty of 10% of the subscription fee per calendar quarter in which the Availability was not achieved, up to a maximum of € 1,000.00 (thousand euro) per calendar quarter.

A ANNEX REGISTRATION FORM ESCROW BENEFICIARY

ESCROW4ALL INFORMATION			
SUPPLIER	Otherside B.V.	Sales Consultant	Timo van Ling
CONTRACT NUMBER	SW2P15399	Contact details	Timo.vanLing@escrow4all.com

Information required for registration of Escrow Beneficiary under an Escrow4all Master Agreement

Details of Beneficiary

Company name
Department
Visiting address
Postal code
Location
Telephone number
Postal Address
Postal code
Location
Country

Contact person

Name
Job title
Telephone number
Email

2nd contact person (optional)

Name
Job title
Telephone number
Email

Specific information

Start participation	Immediately
Product	Xpert Suite
Version	Latest version
Comments	

Please complete the form and email it to: sales@escrow4all.com

The registration will, after assessment, be processed within 5 working days.