RISMAgrc – Online Services Terms and SLA

Table of Contents

Introduction

This document describes the online service terms covering the RISMAgrc / RISMAbusiness suite of applications, namely RISMAactions, RISMAcontrols, RISMArisk and Compliance modules, e.g. GDPR (hereafter referenced RISMAbusiness).

Change History

Version	Date	Description
1.0	01 January 2016	Formal description of the terms and conditions defined for privacy and security. Includes reference to the latest Online Services Terms from Microsoft Inc., which RISMA uses for hosting of our services (Microsoft Azure services).
1.1	01 June 2016	Updated with chapter covering the Risma Service Level Details.
1.2	23 November 2016	Customer Discontinuation Service chapter added to describe how we manage exit of the RISMAbusiness service.
1.3	15 March 2017	Details on Customer Database Backup routine is added.
1.4	9 November 2017	Compliance modules added to RISMAbusiness suite. Newest OST version will become valid upon renewal of license period or if additional subscriptions are purchased. GDPR section added. Reference to RISMAstealth added under Security section. Data at rest location defined. Various simplifications.
1.5	25 May 2018	EU GDPR replacing prior legislation and sections removed which either referenced prior law or which is now covered by our Data Processor Agreement.
1.6	13 September 2018	Added SLA info for customer services in incident management chapter.
1.7	22 March 2019	Added reference to RISMA Systems ISAE 3402-I audit statement.

General Terms & Definitions

Customer may use the Online Services and related software as expressly permitted in Customer's licensing agreement and RISMA Systems A/S (hereafter referenced RISMA) reserves all other rights. Customer must acquire and assign the appropriate subscription licenses required for its use of each application offered.

If any of the terms below are not defined in Customer's licensing agreement, they have the definitions below.

- "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to RISMA by, or on behalf of, Customer through use of RISMAbusiness.
- "External User" means a user of RISMAbusiness that is not an employee, onsite contractor, or onsite agent of Customer or its Affiliates.
- "Instance" means an image of software that is created by executing the software's setup or install procedure or by duplicating such an image.

- "Non-Risma Product" means any third-party-branded software, data, service, website or product.
- "Online Service" means a RISMA-hosted service to which Customer subscribes under a RISMA licensing agreement.

Online Service Term (OST) Updates

The version of the OST at purchase date is valid for the subscription period (i.e. a year).
When Customer renews current set of licenses or purchases additional subscriptions to RISMAbusiness, the current OST will apply.

Regulatory Changes & International Availability

RISMA may make commercially reasonable changes to RISMAbusiness from time to time.
RISMA may terminate the RISMAbusiness service in any country where RISMA is subject to a government regulation, obligation or other requirement that is not generally applicable to businesses operating there.

License Reassignment

A User license is restricted to a number of Users, as described in the License Agreement. A User login must only by used by the named User and must not be shared among several Users. Customer may freely re-assign a User License to another User (by de-activating the prior User).

Data Retention & Deletion

Except for free trials, and unless otherwise agreed, RISMA will retain Customer Data stored in the Online Service in a limited function account for 30 days after expiration or termination of Customer's subscription so that Customer may extract the data.

After the 30-day retention period ends, RISMA will disable Customer's account and delete the Customer Data. RISMA has no liability for the deletion of Customer Data as described in this section.

Non-RISMA Products

RISMA may make Non-RISMA Products available to Customer through Customer's use of the Online Services. If Customer installs or uses any Non-RISMA Product with an Online Service, Customer may not do so in any way that would subject RISMA's intellectual property or technology to obligations beyond those expressly included in Customer's licensing agreement.

For Customer's convenience, RISMA may include charges for the Non-RISMA Product as part of Customer's bill for Online Services. RISMA, however, assumes no responsibility or liability whatsoever for the Non-RISMA Product. Customer is solely responsible for any Non-RISMA Product that it installs or uses with an Online Service.

Acceptable Use Policy

Neither Customer, nor those that access an Online Service through Customer, may use an Online Service:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;

- to spam or distribute malware;
- in a way that could harm the Online Service or impair anyone else's use of it; or
- in any application or situation where failure of the Online Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage.

Violation of the terms in this section may result in suspension of the Online Service. RISMA will suspend the Online Service only to the extent reasonably necessary. Unless RISMA believes an immediate suspension is required, RISMA will provide reasonable notice before suspending an Online Service.

Compliance with Laws

RISMA will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, RISMA is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. RISMA does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to privacy, data protection and confidentiality of communications. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls, and for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation.

Electronic Notices

RISMA may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that RISMA identifies. Notice is given as of the date it is made available by RISMA.

Font Components

While Customer uses an Online Service, Customer may use the fonts installed by that Online Service to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts and temporarily download them to a printer or other output device to print content.

General Privacy and Security Terms

Scope

The terms in this section apply to all Online Services from RISMA, which are governed by the privacy and/or security terms referenced below.

Processing of Personal Data (GPDR)

Article 28(1) of the European Union General Data Protection Regulation ("GDPR") requires an agreement between a controller and processor, and between a processor and sub-processor, that

processing be conducted in accordance with technical and organizational measures that meet the requirements of the GDPR and ensure the protection of the rights of data subjects.
As part of the contractual setup with a Customer, a Data Processor Agreement will be entered.

RISMA is committed to the GDPR Terms towards all customers effective from May 25, 2018.

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. RISMA will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. RISMA acquires no rights in Customer Data, other than the rights Customer grants to RISMA to provide the Online Services to Customer. This paragraph does not affect RISMA's rights in software or services RISMA licenses to Customer.

Debugging using Customer Data

RISMA personnel only access Customer Data with prior authorization from Customer. For debugging purposes, in seldom cases, it might be necessary to include a copy of the Customer database in such analysis (e.g. database corruption or other misbehaviour). After conclusion of the debugging endeavour, the copy of the Customer database will be deleted. The data stored by RISMA personnel are obligated to maintain the security and secrecy of any Customer Data and this obligation continues even after their engagements end.

Disclosure of Customer Data

RISMA will not disclose Customer Data outside of RISMA or its controlled subsidiaries and affiliates except

a. as Customer directs,
b. as described in the OST, or
c. as required by law.

RISMA will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts RISMA with a demand for Customer Data, RISMA will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, RISMA will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Customer Data, RISMA will promptly notify Customer unless prohibited by law. RISMA will reject the request unless required by law to comply. If the request is valid, RISMA will attempt to redirect the third party to request the data directly from Customer.

RISMA will not provide any third party:

a. direct, indirect, blanket or unfettered access to Customer Data;
b. platform encryption keys used to secure Customer Data or the ability to break such encryption; or
c. access to Customer Data if RISMA is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, RISMA may provide Customer's basic contact information to the third party.

Educational Institutions

Customer understands that RISMA may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of RISMA to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in RISMA's possession as may be required under applicable law.

IT Security / RISMAstealth

RISMA is committed to helping protect the security of Customer's information. RISMA has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

RISMA offers Customers with special security needs an additional set of optional security services described in our RISMAstealth package.

Security Incident Notification

If RISMA becomes aware of any unlawful access to any Customer Data stored on RISMA's equipment or in RISMA's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), RISMA will promptly

a. notify Customer of the Security Incident;
b. investigate the Security Incident and provide Customer with detailed information about the Security Incident; and
c. take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means RISMA selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. RISMA's obligation to report or respond to a Security Incident under this section is not an acknowledgement by RISMA of any fault or liability with respect to the Security Incident.

Customer must notify RISMA promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Incident Management by Risma

In case a customer encounters a problem with using the RISMAbusiness service, the user is welcome to raise a problem report including a short description of the problem. Please use the guideline described at our support site: https://support.rismasystems.com/

The user may send RISMA an e-mail to support@rismasystems.com including

- A problem title
- A short problem description,
- The URL of the page where the problem is encountered
- If relevant, a screenshot of the page

As a response to this, RISMA will return to the user within 8 hours with an estimate of when the defect will be fixed (in more complex cases) or simply announce that the problem is fixed.

General opening hours and service level

- Support phone: Open workdays from 9 am to 4 pm. (UTC +1)
- Outside work hours: +45 53541566 (Customer Success director Gitte Barsøe Pedersen)
- Support desk (support@rismasystems.com): Response time within one workday.
- Implementation sessions online or onsite: within 5 workdays.

Location of Customer Data at Rest

RISMA does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

As a consequence, if Customer decides to enable a particular RISMAbusiness service to be deployed within a geographic area (Geo), this does not affect the way in which RISMA stores Customer Data.

Customer data at rest is Microsoft's West-Europe location (The Netherlands).

Backups (encrypted) are additionally placed in Amazons AWS services - data at rest in: EU Central1, (Frankfurt, Germany).

Location of Data Processing

Except as described elsewhere in the OST, Customer Data that RISMA processes on Customer's behalf may be transferred to, and stored and processed in, Denmark or any other EU country in which RISMA or its affiliates or subcontractors maintain facilities. Customer appoints RISMA to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services.

RISMA abides by the requirements of European Economic Area data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area.

RISMA will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. Upon the start of enforcement of the GDPR, RISMA will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate

safeguards as described in Article 46 of the GDPR and that such transfers and safeguards are documented according to Article 30(2) of the GDPR.

Preview Releases

RISMA may offer preview, beta or other pre-release features, data center locations, and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Online Service.

Use of Subcontractors

RISMA may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services RISMA has retained them to provide and will be prohibited from using Customer Data for any other purpose. RISMA remains responsible for its subcontractors' compliance with RISMA's obligations in the OST. Customer has previously consented to RISMA's transfer of Customer Data to subcontractors as described in the OST.

Information Security

General Practices

RISMA has implemented and will maintain and follow for the Online Services the following security measures, which, in conjunction with the security commitments in the OST, are RISMA's only responsibility with respect to the security of Customer Data. The table below specifies different domain approaches. Where RISMA is mentioned, this also includes the 3'rd party hosting service which RISMA will be using to provide the online services.

ISAE-3402-I

RISMA Systems A/S has a ISAE-3402 type 1 auditor declaration pr. March 22nd 2019. This describes the documented policies and procedure that RISMA follows to ensure information security internally and externally. The audit was performed by REVI-IT A/S and the full report is available upon request.

Domain	Practices
Organization of Information Security	**Security Ownership**. RISMA has appointed a security officer responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. RISMA personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. RISMA performs a risk assessment before processing the Customer Data or launching the Online Services service. RISMA retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. RISMA maintains an inventory of all media on which Customer Data is stored within RISMA premises. Access to the inventories of such media is restricted to RISMA personnel authorized in writing to have such access. When Customer Data is hosted with 3'rd party, similar conditions exist for the hosting partner. **Asset Handling** - RISMA classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - RISMA imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - RISMA personnel must obtain RISMA authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside RISMA's facilities.
Human Resources Security	**Information Security Training**. RISMA informs its personnel about relevant information security policies and procedures and their respective roles. RISMA also informs its personnel of possible consequences of breaching the

Domain	Practices
	security rules and procedures. RISMA will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. RISMA limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components**. RISMA maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **Protection from Disruptions**. RISMA uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. RISMA uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy** RISMA maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a day (unless no Customer Data has been updated during that period), RISMA maintains multiple copies of Customer Data from which Customer Data can be recovered. - RISMA stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - RISMA has specific procedures in place governing access to copies of Customer Data. - RISMA reviews data recovery procedures at least every twelve months. - RISMA logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software** RISMA has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - RISMA encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - RISMA restricts access to Customer Data in media leaving its facilities.

Domain	Practices
	Event Logging RISMA logs access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy** RISMA maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - RISMA maintains and updates a record of personnel authorized to access RISMA systems that contain Customer Data. - RISMA deactivates authentication credentials that have not been used for a period of time not to exceed six months. - RISMA identifies those personnel who may grant, alter or cancel authorized access to data and resources. - RISMA ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - RISMA restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - RISMA instructs RISMA personnel to disable administrative sessions when leaving premises RISMA controls or when computers are otherwise left unattended. - RISMA stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - RISMA uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, RISMA requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, RISMA requires the password to be at least eight characters long. - RISMA ensures that de-activated or expired identifiers are not granted to other individuals. - RISMA monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - RISMA maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

Domain	Practices
	- RISMA uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design** RISMA has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - RISMA maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by RISMA (as described in the "Security Incident Notification" section above) will be made without unreasonable delay and, in any event, within 72 hours. **Service Monitoring** RISMA security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- RISMA maintains emergency and contingency plans for the facilities in which RISMA information systems that process Customer Data are located. - RISMA's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Online Services Information Security Policy

The hosting company selected by RISMA to provide the Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below. For further details, please refer to the Microsoft Online Services Terms.

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice
Microsoft Azure	Yes	Yes	Yes

RISMA may add industry or government standards at any time. RISMA will not eliminate a standard or framework in the table above, unless it is no longer used in the industry and it is replaced with a successor (if any).

Risma Service Level Agreement

This section describes the service level agreement covering the Microsoft Azure service used for providing the RISMAbusiness solution as well as how RISMA manages costumer found defects.

Microsoft Azure Cloud Service

The specific service levels (up-time etc.) are described in detail here:
http://azure.microsoft.com/support/legal/sla/
Select Virtual machines as the specific service.

RISMAbusiness database backup

Customer databases are backed up on a daily basis and are kept for 3 months. Monthly versions are kept for a year.
Backups are encrypted at file level as well as server level (2 step encryption).
Backups are stored both in Azure as well as Amazon Web Services to ensure an Azure service independent backup facility.

RISMAbusiness Service Update

In case of updating a version of the RISMAbusiness solution, normal down-time is less than 5 minutes and is usually performed outside normal business hours – or agreed with the customer directly. In case that a longer period is required, the timing of this will be agreed with the Customer.

Customer Discontinuation Service

If the customer decides to discontinue use of RISMAbusiness, and wishes to re-use the data built up during the use of the service, RISMA offers a Discontinuation service where either

1) The RISMAbusiness service is continued for a period agreed in order to allow transfer of data

or

2) An export of the Customer database, which contains all data created during the use of RISMAbusiness, including uploaded files
3) Engineering Support is provided to read and understand the database structure and associated tables.

How to Contact RISMA

If Customer believes that RISMA is not adhering to its privacy or security commitments, Customer may contact customer support.

RISMA's mailing address is:

RISMA Systems A/S
Att. Customer Success
Lyskaer 8
DK-2730
Denmark