Data Processing Agreement
Sol Inventum OÜ - SecureMailMerge

This Data Processing Agreement (“Agreement“) forms part of the Contract for

Services (“Principal Agreement“) between

Sol Inventum OÜ
Sepapaja tn 6,
Lasnamäe linnaosa,
15551 Tallinn, Harju maakond
Estonia
Company Nr: 14665482

Email for notices:

Email for notices:

office@solinventum.com

(the “Company”)

(the “Data Processor”)

(together as the “Parties”)

This Agreement relates to the Company’s use of SecureMailMerge, the Service further described in Annex 1.

WHEREAS

(A) The Company acts as a Data Controller.
(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.
(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
(D) The Parties wish to lay down their rights and obligations.

DRAFT

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 “Agreement” means this Data Processing Agreement and all Annexes hereto;

1.1.2 “Company Personal Data” means any Personal Data Processed by the Data Processor or a Contracted Processor on behalf of the Company pursuant to or in connection with the Principal Agreement;

1.1.3 “Contracted Processor” means the Data Processor or a Subprocessor;

1.1.4 “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 “EEA” means the European Economic Area;

1.1.6 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.8 “CCPA” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations;

1.1.9 “Data Transfer” means:

1.1.9.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.9.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subprocessor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.10 “Services” means SecureMailMerge, a Microsoft Outlook add-in, provided by the Data Processor to the Company under the Principal Agreement and further described in Annex 1;

DRAFT

1.1.11 “Subprocessor” means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.1.12 “Applicable Laws” means all laws, regulations and binding regulatory guidance applicable to a Party in the performance of this Agreement, including the Data Protection Laws.

1.2 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

DRAFT

2.1 Data Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company’s documented instructions, including with regard to transfers of Company Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest; and

2.1.3 immediately inform the Company if, in its opinion, an instruction given by the Company infringes the GDPR or any other Union or Member State data protection provision.

2.2 The Company instructs the Data Processor to Process Company Personal Data only as necessary to provide the Services, as described in Annex 1, and otherwise on the Company’s documented instructions. Annex 1 constitutes the Company’s initial documented instructions.

2.3 The Parties acknowledge and agree that Data Processor is a service provider for the purposes of the CCPA (to the extent it applies) and is receiving personal information from the Company in order to provide the Services, which constitutes a business purpose.

2.3.1 Data Processor shall:

2.3.1.1 not sell or share any such personal information; and

2.3.1.2 not retain, use or disclose any personal information provided by Company pursuant to the Agreement (i) except as necessary for the specific purpose of performing the Services for Company pursuant to the Agreement, or otherwise as set forth in the Agreement or as permitted by the CCPA; (ii) or outside the direct business relationship between Company and Data Processor; and

2.3.1.3 not combine personal information that the Data Processor receives from, or on behalf of, Company with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, except to perform any business purpose.

2.3.2 Company is responsible for ensuring its compliance with the requirements of the CCPA in its use of the services and Deliverables Data Processor provides to Company and its own processing of personal information.

2.3.3 The Parties acknowledge and agree that the exchange of Personal Information between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Services or the Agreement.

2.3.4 Data Processor certifies and acknowledges that (i) it understands the restrictions set forth in this section 2.3 and will at all times comply with them; (ii) it will comply with the applicable obligations under the CCPA, and shall provide the same level of privacy protection as is required by the CCPA; (iii) Company shall be permitted to take reasonable and appropriate steps to help ensure that Data Processor uses personal information in a manner consistent with Company's obligations under the CCPA; (iv) it will notify Company if it makes a determination that it can no longer meet its obligations under the CCPA; and (v) Company shall, upon notice, including any such notice provided under (iv) above, be permitted to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information;

2.3.5 The terms "business purpose", "personal information", "service provider", "sale", and "sell" used in this section 2.3 are as defined in the CCPA.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know /

DRAFT

access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3 The technical and organisational measures implemented by the Data Processor as at the date of this Agreement are set out in Annex 3. The Data Processor may update those measures from time to time provided that the level of security is not thereby reduced.

4.4 The Data Processor warrants that the Services are designed such that the Company's recipient data, merge-field content and message content are Processed exclusively on the Company's own devices and within the Company's own Microsoft 365 tenant, and are not, in the course of the Company's use of the Services, transmitted to, stored on, or accessible by any system controlled by the Data Processor or any Subprocessor. The only Personal Data transmitted to the Data Processor in the course of the Company's use of the Services is that set out in Annex 1.

4.5 The warranty in section 4.4 does not extend to material that a user of the Company voluntarily submits to the Data Processor outside the Services, for example by attaching a data source file to a support request. Any such material is Processed as support correspondence in accordance with Annex 1, and the Company shall instruct its users not to submit Personal Data to the Data Processor's support channel beyond what is necessary to resolve the request.

DRAFT

5. Subprocessing

5.1 The Company grants the Data Processor a general authorisation to engage the Subprocessors listed in Annex 2. The Data Processor shall not appoint (or disclose any Company Personal Data to) any other Subprocessor without giving the Company at least 30 days' prior written notice, during which period the Company may object on reasonable data protection grounds. Where the Company objects and the Parties cannot agree a resolution, the Company may terminate the affected Services.

5.2 The Data Processor shall ensure that each Subprocessor is engaged under a written contract imposing data protection obligations no less protective than those set out in this Agreement, and remains fully liable to the Company for the performance of each Subprocessor's obligations.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient

DRAFT

information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Company Personal Data

9.1 Subject to this section 9, Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the “Cessation Date”), delete and procure the deletion of all copies of those Company Personal Data, or, at the Company’s written election made before the Cessation Date, return those Company Personal Data to the Company and then delete all remaining copies.

9.2 The Data Processor may retain Company Personal Data to the extent, and for so long as, required by Applicable Laws, provided that it ensures the confidentiality of that Company Personal Data and Processes it only for the purposes for which retention is required.

9.3 Company Personal Data contained in routine backup media is deleted in accordance with the Data Processor’s backup rotation cycle as described in Annex 3, and until such deletion remains subject to the confidentiality and security obligations of this Agreement. The Data Processor shall not restore such backups other than for disaster recovery purposes. Where a backup is restored, the Data Processor shall audit the restored data against deletions of Company Personal Data made since that backup was taken, and shall re-apply those deletions without undue delay.

DRAFT

9.4 Notwithstanding section 9.1, the Data Processor may retain the account login identifier and email address of the Company's users after the Cessation Date, for the sole purpose of preventing abuse of, and fraud against, the Services. In respect of that retention the Data Processor acts as a controller on the basis of its legitimate interests. It shall retain no other category of Company Personal Data on that basis, shall not use the retained data for any other purpose, and shall not disclose it except as required by law.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

DRAFT

11. Data Transfer

11.1 The Data Processor may not transfer or authorise the transfer of Company Personal Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. The Company's execution of this Agreement constitutes that consent in respect of, and only in respect of, the Subprocessors and transfers described in Annex 2. Where Company Personal Data is transferred from a country within the EEA to a country outside the EEA, the Parties shall ensure that it is adequately protected by the transfer mechanism identified for the relevant Subprocessor in Annex 2.

12. Mergers, Sale, or other asset transfer.

12.1 The Data Processor shall not sell, licence, transfer or otherwise dispose of Company Personal Data as a standalone asset of its business.

12.2 A change in the ownership or control of the Data Processor, including a sale of its shares, does not of itself constitute a transfer of Company Personal Data, and this Agreement continues in force unaffected.

12.3 Where the business or assets to which the Services relate are transferred to a successor entity, whether by merger, acquisition, reorganisation, insolvency or comparable transaction, Company Personal Data may be transferred to that successor only for the continued provision of the Services and only subject to this Agreement. The Data Processor shall notify the Company without undue delay following completion. The successor shall not Process Company Personal Data for any purpose other than those set out in Annex 1 without the Company's documented instructions.

12.4 The Data Processor may disclose information relating to this Agreement to a prospective acquirer and its professional advisers under written obligations of confidentiality, provided that such disclosure is limited to what is reasonably necessary for the transaction and that Company Personal Data is disclosed only in anonymised or aggregated form unless the Company agrees otherwise in writing.

13. General Terms

13.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

13.2 Notices

All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the postal address or email address set out in the heading of this Agreement, or to such other address as a Party notifies from time to time. Notices under section 5.1 may be given by email to the Company's address for notices.

DRAFT

14. Governing Law and Jurisdiction

14.1 This Agreement is governed by the laws of Estonia.

14.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Estonia.

DRAFT

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

The Company

Name:

Title:

Signature:

Date Signed:

The Data Processor

Name:

Title:

Signature:

Date Signed:

DRAFT

Annex 1 – Details of the Processing

This Annex forms part of the Agreement and sets out the particulars required by Article 28(3) GDPR.

Service in scope	SecureMailMerge, a Microsoft Outlook add-in distributed via Microsoft AppSource.
Subject matter	Licensing, provision and support of the SecureMailMerge add-in, which enables the Company's users to compose and send personalised email messages from their own Microsoft 365 mailboxes.
Duration of the Processing	The term of the Principal Agreement, plus the period provided for in section 9 of the Agreement.
Nature of the Processing	All parsing of the Company's data source, merge-field substitution and message generation are performed locally within the user's Outlook client on the user's own device. Generated messages are transmitted only to the Company's own Microsoft 365 tenant (Microsoft Graph) for sending. The Processing carried out by the Data Processor is limited to the storage and use of licence and account data on the Data Processor's licensing server (licensing.solinventum.com) for the purpose of issuing and validating licences.
Purpose of the Processing	To issue, validate and administer licences for the Services, and to respond to support requests. The Data Processor does not use Company Personal Data for product improvement, advertising, profiling or the training of machine-learning models.
Type of Personal Data Processed by the Data Processor	Licence and account data held on the licensing server: the licensee's email address, name and Microsoft user identifier, a read-only Microsoft Graph access token, and the associated licence key and subscription status. Support correspondence submitted by a user to the Data Processor's support channel, and its contents. Cookieless usage statistics (frequency of use and number of messages sent). These are collected in aggregate and are not attributable to an individual; they are listed here for transparency and are not treated by the Data Processor as Personal Data. Technical error diagnostics (code location, error type and diagnostic information) where an application error occurs. The read-only Microsoft Graph access token permits the retrieval of the licensee's own profile information only. It does not confer access to the licensee's mailbox. The token used by the add-in to

DRAFT

	send messages is held on the user's own device and is transmitted only to Microsoft Graph.
Personal Data NOT Processed by the Data Processor	Recipient names, recipient email addresses and all merge-field values contained in the Company's data source; message subject lines, message bodies and attachments; campaign data held in the add-in's local storage on the user's device. In the course of the Company's use of the Services, such data is at no time transmitted to, stored on, or accessible by any system controlled by the Data Processor or any Subprocessor. See sections 4.4 and 4.5 of the Agreement. The sole exception is material that a user voluntarily submits to the Data Processor's support channel, for example by attaching a data source file to a support request. Such material is Processed as support correspondence and is subject to the retention position stated below. The Services do not track message opens or clicks and provide no campaign analytics. No open, click or delivery tracking data relating to recipients is generated or stored.
Categories of Data Subject	The Company's employees and other individuals to whom the Company allocates a licence for the Services, and who contact the Data Processor's support channel.
Special categories of Personal Data	The Services are not designed for, and the Data Processor does not request, Personal Data falling within Article 9 GDPR or Article 10 GDPR. No such data is transmitted to the Data Processor in the course of the Company's use of the Services. The Data Processor cannot control the content of material a user voluntarily submits to its support channel. The Company shall ensure that its users do not submit Personal Data falling within Article 9 GDPR or Article 10 GDPR to that channel. See section 4.5.
Frequency of the Processing	Continuous, for the duration of the Principal Agreement.
Storage location	Microsoft Azure, European Union data centres. Website and add-in code is delivered through Cloudflare's content delivery network.
Retention	Licence and account data: retained for as long as the licence remains active. Where an account is deleted during the term, that data is deleted at most 30 days after account deletion. On the Cessation Date, deletion takes place within the period stated in section 9.1, save for records the Data Processor is required to retain under applicable accounting or tax law (section 9.2). Copies of licence and account data persist in backup media after deletion from live systems for no longer than 12 months, in accordance with Annex 3 and section 9.3. The Data Processor may retain the account login identifier and email address of the Company's users beyond those periods for the sole purpose of preventing abuse of, and fraud against, the

DRAFT

	Services, in accordance with section 9.4. Support correspondence, and any material a user voluntarily attaches to it, is retained in the Data Processor's support ticketing system for the duration of the support relationship; no automated retention limit is applied during that period. Such correspondence is deleted at any time on request by the Company or the data subject, and in any event on the Cessation Date in accordance with section 9. Save as stated above, no recipient, merge-field or message data is received or retained.
Billing and payment data	Billing and payment data is collected and Processed by the Data Processor's merchant of record, or by Microsoft where the Company purchases through its Microsoft 365 invoice. Those providers act as controllers of that data under their own privacy policies and terms. Billing and payment data is outside the scope of this Agreement and is not Processed by the Data Processor on the Company's behalf.
Transfers outside the EEA	Licence and account data is stored within the EU. Transfers arise only in respect of the Subprocessors identified in Annex 2 as located outside the EEA, subject to the safeguards stated there.

DRAFT

Annex 2 – Approved Subprocessors

The Company authorises the Data Processor to engage the Subprocessors listed below, in accordance with section 5 of the Agreement.

Subprocessor	Purpose	Location	Transfer safeguard
Microsoft Ireland Operations Limited	Contracting entity. Cloud hosting and database infrastructure (Azure) for the licensing server	EU	N/A (EU). See note below on Microsoft Corporation
Microsoft Corporation	Parent undertaking of Microsoft Ireland Operations Limited. Remote engineering and support access to EU-hosted systems, global security operations, support case escalation, service telemetry and subscription licence validation, as described in Microsoft's published EU Data Boundary documentation	United States, and other regions worldwide for security operations	Microsoft Data Protection Addendum incorporating EU SCCs; EU-US Data Privacy Framework
Cloudflare, Inc.	Hosting and delivery of website and add-in code, forwarding of licence-check requests to the licensing server, storage of pseudonymous advertising click identifiers in Cloudflare D1	Global edge network, US-headquartered	EU SCCs – Module 3; EU-US Data Privacy Framework
Functional Software, Inc. (Sentry)	Application exception logging: code location, error type and technical	US	EU SCCs – Module 3

DRAFT

	diagnostic information		
Help Scout PBC	Customer support ticketing and correspondence	US	EU SCCs – Module 3
Resend, Inc.	Transactional email sent from the licensing portal, including licensee names and email addresses	US	EU SCCs – Module 3

The transfer mechanism applicable to each Subprocessor is stated in the table above. Where that mechanism is an adequacy decision, no further transfer instrument is required. Where it is the EU-US Data Privacy Framework, the Data Processor relies on the recipient's certification under that Framework. Where it is standard contractual clauses, the Data Processor has entered into the European Commission's standard contractual clauses (Decision (EU) 2021/914), Module Three (processor to sub-processor), with the relevant Subprocessor, together with any supplementary measures identified by a transfer impact assessment.

Microsoft Ireland Operations Limited is the contracting entity and hosts the infrastructure within the European Union. It is a subsidiary of Microsoft Corporation, a United States undertaking. Microsoft's published EU Data Boundary documentation records that certain categories of data continue to be accessed from, or transferred outside, the EU Data Boundary, including remote access by engineering and support personnel located outside the EU, global security operations, technical support case titles and the content of escalated support cases, limited directory data, variable network routing, and subscription licence validation. Those transfers are governed by Microsoft's Data Protection Addendum incorporating the EU standard contractual clauses. No recipient, merge-field or message content is disclosed to any Subprocessor listed above.

Other recipients (not Subprocessors)

The recipients below are listed for transparency and are not Subprocessors of Company Personal Data. Billing and payment data is Processed by Paddle, or by Microsoft where the

DRAFT

Company purchases through its Microsoft 365 invoice, in each case as a controller under that provider's own privacy policy and terms; see Annex 1. Usage statistics are processed on a server operated by the Data Processor, hosted by Hetzner Online GmbH (EU). No third-party analytics provider receives them.

Subprocessor	Purpose	Location	Transfer safeguard
Paddle.com Market Ltd	Merchant of record: subscription billing and payment processing. Acts as a controller of billing and payment data under its own privacy policy	United Kingdom	UK adequacy decision
Microsoft Corporation (AppSource / Partner Center)	Billing where the Company purchases through its Microsoft 365 invoice. Acts as a controller of billing and payment data under its own privacy policy	EU / US	EU-US Data Privacy Framework

DRAFT

Annex 3 – Technical and Organisational Measures

The measures below are those implemented by the Data Processor pursuant to Article 32 GDPR and section 4 of the Agreement.

Pseudonymisation and encryption (Art. 32(1)(a))	Data in transit is exchanged over TLS-secured channels and protected with digital signatures. All databases operated by the Data Processor are encrypted at rest.
Confidentiality (Art. 32(1)(b))	Access follows the principle of least privilege. Staff access to the licensing server is granted through Microsoft 365 Authentication. All personnel with access to Company Personal Data are bound by written confidentiality undertakings.
Integrity (Art. 32(1)(b))	Source code is maintained in a version-controlled repository with change history. Changes are reviewed prior to deployment to production. Audit logging of administrative actions and access is enabled on the licensing server.
Availability and resilience (Art. 32(1)(b))	Infrastructure is operated in Microsoft Azure data centres within the European Union. A point-in-time and long-term backup strategy is applied to the licensing database. Backup media is retained for no longer than 12 months, after which it is overwritten. This is the backup rotation cycle referred to in section 9.3. Company Personal Data held in backup media is not accessed or otherwise Processed except for disaster recovery.
Restoration of availability (Art. 32(1)(c))	Restoration is performed using the managed point-in-time and long-term backup facilities of Microsoft Azure described above. Scheduled disaster recovery exercises are not currently performed.
Regular testing and evaluation (Art. 32(1)(d))	Automated dependency and vulnerability scanning of the code base is in place, and Microsoft Publisher Attestation is completed and published for the Services. Third-party penetration testing is not currently performed. The Data Processor relies on the certified infrastructure and platform controls of Microsoft Azure and Cloudflare, as set out below, together with a reduced attack surface arising from the on-device processing model described in this Annex.
Data minimisation by design	All campaign processing occurs on the user's own device: the Data Processor operates no server that processes campaigns, and recipient, merge-field and message content is never transmitted to it. See sections 4.4 and 4.5 of the Agreement and Annex 1.

DRAFT

Subprocessor assurance	Cloudflare, Inc. maintains ISO 27001, ISO 27018, ISO 27701 and SOC 2 Type II certification. Microsoft Azure operates under its own published certification programme. The Data Processor itself does not currently hold SOC 2 or ISO 27001 certification.
Personal data breach management	Documented breach detection, assessment and notification procedure, aligned to the notification obligation in section 7 of the Agreement.

DRAFT