DPA ENCLOSURE – Scrive eSign

Annex I – Processing Activities

1 Purposes of Processing

The processor shall, in accordance with the Agreement, provide the controller with:

(i) Scrive eSign, i.e. a cloud-based software as a service solution used by controller for the main purposes of performing and/or enabling; electronic signatures of documents provided by the controller; various methods for authentication of a signatory's identity;

(ii) the optional storing of documents, including related evidence materials within the solution, and;

(iii) associated support/maintenance/statistical/security services, including problem report handling services.

All of the above is hereinafter referred to as the "Services".

2 Instructions

a. The processor shall only be entitled to process the personal data for the purposes set out in section 1 above, for the duration of the Agreement, and in accordance with the controller's reasonable written instructions, and in any event in compliance with applicable laws and legal obligations. In this context, the processor's provision of the Services in accordance with the controller's configurations of, and data input into, Scrive eSign shall be deemed as following the instructions from the controller. If, by following any additional reasonable instructions from the controller, the processor would incur additional costs (other than such costs that the processor incurs as a result to amend necessary operations in order for it to comply with the GDPR), the Parties shall agree in good faith on the apportionment of such costs.

b. Controller acknowledges and agrees that (i) a Processed Document can be sent/made available through the Services via e-mail, SMS or touch device to such third party recipient(s) as designated by controller and that the recipient may thus access the Processed Document from whatever country where the recipient may be located; (ii) in the event that such a recipient is/becomes an External User, then such third party also becomes a "data controller" with regards to any Personal Data included in that same Processed Document, and; (iii) Processor may, on behalf of an External User, retain within Scrive eSign any such Processed Documents stored within their separate account, even after the same Processed Documents have been deleted from Controller's own account.

c. Controller acknowledges and agrees that the processor's processing of the controller's personal data in the context of providing support/maintenance/statistical/security services, including problem report handling services shall be solely governed by the Agreement, including the Clauses, notwithstanding that the Reseller is responsible for providing controller with first line support, and that the Reseller may forward and receive controller's personal data to/from processor in this context.

3 Specific Definitions

"**External Initiator**"	means a third party that initiates a signing process via the Services for a specific Processed Document. N.b. a third party can only initiate a signing process via the Services if the controller has enabled such access via an integration with the Scrive eSign service (typically as a web-form integration).
"**External User**"	means a third party that has an active account of their own within Scrive eSign. To avoid doubt; also an employee of the controller could, in their capacity of a private person with a private account in Scrive eSign, be deemed as an External User.
"**Initiator**"	means an individual employee/representative of the controller that initiates a signing process via the Services for a specific Processed Document.

"**Flow Process**"	means a Scrive eSign Flow process containing one or more Processed Documents.
"**Processed Document**"	means a document that has been uploaded to Scrive eSign by the controller by any available means (e.g. Scrive eSign web-interface, API or printer-driver) and including any and all personal data that is (i) included in such document and (ii) associated therewith as metadata.

4 Categories of data subjects

a) Any data subject that acts as the Initiator in relation to a Processed Document;
b) Any data subject as may be designated by the Initiator as a signatory, reviewer, or other party, in relation to a Processed Document (including any data subject that meets the Initiator's search criteria in a connected system such as a contact book);
c) Any data subject that acts as an External Initiator in relation to a Processed Document, and;
d) Any other data subject (if any) whose personal data was originally included in the contents of a Processed Document - or as may be added to a Processed Document by a signatory thereto - without such data subject belonging to either of the above categories with regards to that same Processed Document.
e) Employees of the controller that have an account in the Services and/or that contact the processor's support/helpdesk resources.

5 Categories of personal data

(i) Always Audit trail / evidence collected to ensure the validity of electronic signatures, including time of reviewing and signing, and IP-addresses of the parties involved in the individual signing process.
(ii) Typically Name and contact details (e.g., email address, home address, mobile phone number etc.) of the data subject that shall be the signatory or reviewer of a Processed Document. Handwritten signature (optional). In case eID is used (optional); any such categories of personal data as processed by/returned from the selected eID Provider, as further detailed in Annex II.
(iii) Additionally Any other personal data that may be added by an Initiator/External Initiator of a Processed Document and/or originally included in the Processed Document, and/or added or attached to the Processed Document by a signatory to the document.

6 Processing Operations

The Processing of personal data in accordance with the Agreement includes the following main events:

1. Personal data of category (i) Always is collected by the Services throughout all events and gathered in an event log (audit trail) that is appended to the Processed Document when signed by all parties thereto.
2. Personal data may already be included in a document to be Processed when uploaded to the Services by the Initiator, or when already made available to the Initiator (or External Initiator, as the case may be) as a template stored in the Services.

3. a) Personal data is added as metadata in the Services by the Initiator and may be used to populate fields in the Processed Document and to designate roles in relation to a Processed Document or a Flow Process. b) In case of use via an integration to the Scrive eSign API: personal data as entered by an Initiator (or External Initiator, as the case may be) is automatically transferred as metadata from the controller's system to the Services and may be used to populate fields in the Processed Document and to designate roles in relation to a Processed Document or a Flow Process. c) Additional personal data may be added, or attached, by a signatory to the Processed Document
4. The Processed Document is made available to the signatories, reviewers or other parties thereto via the means as configured by the controller, i.e. through either a) an invitation message sent via the services (including a hyperlink to the Processed Document) distributed to the designated recipients via email and/or SMS, b) through email and/or SMS services outside of the services or c) without any invitation message in case of e.g. a web-form integration.
5. When the Processed Document has been signed by all the signatories thereto, personal data is embedded in the final PDF, as well as in the attached evidence package. The final PDF, including the evidence package attachments, is sealed with a digital signature, and then retained in the e-archive of the Scrive eSign service together with the metadata associated with the Processed Document.
6. Unless configured otherwise by the controller in the Services, the final PDF is distributed as an attachment via confirmation email to the Initiator, the signatories, and reviewers (if any) of the Processed Document. The final PDF may also/alternatively be distributed and made available (downloadable) via web-link included in confirmation SMS to such parties.

7 Data Retention

Retention and deletion of personal data in the e-archive of the Services:

1. Personal data is retained in the e-archive of the Services in two types of instances; (i) as data included in a Processed Document or template document, and (ii) as metadata related to the Initiator (or External Initiator, as the case may be), each signatory and any reviewer to the Processed Document.
2. Processed Documents, Flow Processes, templates and related metadata will be retained in the e-archive for as long as the controller has not deleted the same through any of the means available via the Services, including events of automatic trashing/deletion in accordance retention settings within the Services.
3. The controller is able to delete Processed Documents, Flow Processes, templates and related metadata either by manual input and settings in the Services, or programmatically via the API of the Services as further described below.
4. a) Deletion of Processed Documents "Trashing". A Processed Document can be initially trashed either: a) manually by the controller within the Services, or via an API call, or; b) automatically within a specific interval as per optional controller specific retention settings for trashing within the Services. When trashed, the Processed Document will be retained in a "trashed state" in the e-archive until the occurrence of the earliest of the following options for deleting.

"Deleting". A trashed Processed Document can be deleted from the e-archive either: a) manually by the controller within the Services, or via an API call; b) within a specific interval (0 - 365 days from when the Processed Document is trashed) as per the controller's retention settings within the Services, or; c) "immediately" (i.e. within 24 hours) if that retention setting within the Services is activated by the controller.[1] If no controller specific setting as per b) or c) is made, the default setting will apply. The default setting is deletion 30 days from trashing.

b) Deletion of Flow Processes

"Trashing". A Flow Process can be initially trashed either: a) manually by the controller within the Services, or via an API call; b) automatically within a specific interval as per optional controller specific retention settings for trashing within the Services, or; c) automatically within an interval specified in the current default settings for trashing within the Services[2].

Option c) applies as default unless either: option b) is used, or; an "indefinite" retention setting has been applied within the Services instead of option c).

When trashed, a Flow Process will be retained in a "trashed state" in the e-archive until the occurrence of the earliest of the following options for deleting:

"Deleting". A trashed Flow Process can be deleted from the e-archive either: a) manually by the controller within the Services, or via an API call; b) within a specific interval (0 - 365 days from when the Flow Process is trashed) as per the controller's retention settings within the Services, or; c) "immediately" (i.e. within 24 hours) if such retention setting within the Services is activated by the controller (as and when available)[1]. If no controller specific setting as per b) or c) is made, the default setting will apply. The default setting is deletion 30 days from trashing.

5.

a) When a Processed Document is deleted, related metadata including any personal data is also deleted by default. N.b. The processor will still retain non-personal data such as the document id (unique transaction number), authentication transaction ids (unique transaction number(s)), authentication provider labels and date & time for sealing of the document for the purposes of billing and maintaining a complete transaction log.

b) When a Flow Process is deleted, the Processed Documents included therein are also deleted by default together with related metadata including any personal data. N.b. The processor will still retain non-personal data such as the Flow Process id, associated document id(s), flow specific participant ids, authentication transaction ids (unique transaction number(s)), authentication provider labels and date & time for the sealing of the Flow Process and the related Processed Documents for the purposes of billing and maintaining a complete transaction log.

In any case, eID transaction data, including personal data, will be retained for 30 days from the start of the eID transaction in a separate log file for support and security purposes. The eID transaction data is thereafter immediately and automatically deleted from the log file.

Retention and deletion of data upon termination of the Agreement:

6. Upon the termination of the Agreement and subject to section 7 below, the processor will delete all of the controller's personal data. The controller may in writing request the processor to return to the controller any retained personal data prior to deleting any remaining copies in accordance with the above. Such request must however be done within ten (10) days after the termination of the Agreement.

[1] N.b. in the event the controller desires to use such "immediately" setting on a company account level this may be configurable only by the processor subject to separate order and charges.
[2] https://scrive.com/flow/documentation/api-reference (see the Data Retention section.)

Retention and deletion of back-up data:

7. Once a Processed Document or template (including related metadata) is deleted from the e-archive, back-up copies of the same will be deleted from the processor's separate encrypted data back-up servers hosted by the processor's back-up provider in accordance with the processor's data retention policy. I.e. back-ups are currently retained for 6 months as from the deletion from the e-archive, where after the back-ups are automatically deleted.

Annex II – Sub-processor list

1. Approved sub-processors

On commencement of these Clauses, the controller authorises the engagement of the sub-processors listed in the tables of this annex.

In addition to sub-processors, this annex contains a table with providers. It is acknowledged by the controller that:

- An eID provider that has issued an eID to a data subject is normally deemed to be a controller - in its own right - of the related personal data, and such an eID provider is thus not considered to process personal data on the behalf of the controller.
- An eID provider (whether being an issuer of an eID, an aggregator/broker of eID services or a provider of identity verification services) may be obliged to retain all, or parts of, any data related to an eID transaction in accordance with a specific regulatory duty or similar, and/or in its capacity of a controller in its own right.
- Thus, the eID provider's policies for retention and deletion of such data as well as processor's contract with the eID provider, may not allow for the controller and/or the processor to issue specific instructions to the eID provider for retention and deletion thereof.
- In such a context where the eID provider is obliged to retain data in lieu of following instructions from the processor and/or is a controller in its own right, the eID provider shall be deemed to determine the purposes and means for any such further processing on its own behalf.

i. Scrive eSign Core Functionality

Sub-Processor	Purpose of the Processing	Categories of personal data	Location
Hosting			
Amazon Web Services	Cloud-hosting of Scrive eSign service	All categories that are processed	Ireland & Germany
Google Cloud Platform	Data back-ups	All categories that are processed	Germany
Notifications			
Flowmailer	Transactional email and SMS services	Names, email addresses, and phone numbers of recipients of notifications sent via the Services N.b. signed documents may be attached.	The Netherlands
Generic	Transactional SMS services	Name and mobile number of recipients of	Sweden

		notifications sent via the Services	
Mailgun	Transactional email services	Name & email address of recipients of notifications sent via the Services N.b. signed documents may be attached.	EU
Sinch	Transactional SMS services	Name and mobile number of recipients of notifications sent via the Services	Ireland & Sweden

ii. Scrive Support Services

Sub-Processor	Purpose of the Processing	Categories of personal data	Location
Freshworks	Support portal	Depends on the contents sent to processor by controller.	European Union
Puzzel	Telephony services for new support portal	Telephone number of controller's staff calling into the support portal.	EU/EEA
Stonly	Help centre and feedback functionality.	Normally name and email address. Any other potential personal data depends on the feedback provided.	France
Google Workspace	Handling support requests	Depends on the contents of emails sent to processor by controller.	Europe[3]
Ebbot	Handling support requests.	Depends on the contents of emails sent to processor by controller	EU/EEA

iii. Optional Add-on Services

Sub-Processor	Purpose of the Processing	Categories of personal data	Location
eID and identity verification services			
Bluem (iDIN)	Provision of electronic identification,	Name, address, phone number, birthdate, gender, Bank Identifier Number	Netherlands

[3] Google Workspace provides the option to choose geographic location to store the data. Scrive has selected the region Europe.

	authentication, and signature services (optional usage)	(BIN). Potentially also telephone number and email.	
Onfido	Provision of electronic identification, authentication and signature services (optional usage)	As specified in the Onfido sub-processor list, including but not limited to: Name, email address, image of identity document, image of the data subject's face and information describing the identity document and biometric data.	As specified in the Onfido sub-processor list.

As stated in the introduction of this annex, the providers listed below are not sub-processors in the meaning of the GDPR. They have been included here for transparency, and to consolidate information on personal data processing in a single location.

Provider	**Purpose of the Processing**	**Categories of personal data**	**Location**
eID and identity verification services			
Nordea (Swedish BankID)	Provision of electronic identification, authentication, and signature services (optional usage)	Name, mobile number, personal identification number.	Sweden
Freja eID Group AB (Freja eID+)	Provision of electronic identification, authentication, and signature services (optional usage)	Name, mobile number, personal identification number	Sweden
BidBax (Norwegian BankID)	Provision of electronic identification, authentication, and signature services (optional usage)	Name, mobile number, personal identification number.	Norway
Nets[4] (Various eIDs such as FTN, and MitID)	Provision of electronic identification, authentication, and signature services (optional usage)	Name, mobile number, personal identification number (or similar)	EU/EEA
Verimi	Provision of electronic identification, authentication, and signature services	Name, mobile number, personal identification number. Potentially also video-identification.	Germany

[4] Refer to the End Customer MitID Terms for further details with regard to MitID.

	(optional usage)		
Belgian Mobile ID (itsme)	Provision of eID based identification, authentication, and signature services (optional usage)	Name, date of birth, phone number, email address, address, nationality, city of birth, national eID (Belgian), device information, photo	Belgium
Swisscom	Provision of electronic identification, authentication, and signature services (optional usage)	Name, mobile number, personal identification number. Potentially also video-identification.	Austria, Switzerland
SK ID Solutions (SmartID)	Provision of electronic identification, authentication, and signature services (optional usage)	Name, personal identification number, for non-Baltic citizens passport or ID-card number, IP address; phone number, and language of communication	Estonia

2. Additional conditions related to the use of sub-processors

Optional usage

The controller accepts and acknowledges that the controller is entrusted with selecting to use such sub-processors that are subject to "optional usage" as per the current sub-processor list. The selection of usage may either be made directly within the Services through controller's own configurations/settings, or - when specific activation is required - by ordering access to the services provided by a specific sub-processor from the processor.

Prior notice for the authorisation of sub-processors

With reference to clause 7.7 (a) the controller may object to such notified change in the event of its reasonable concerns with regards to the appropriate protection of personal data. Such objection shall be detailed in writing within fifteen (15) working days from the processor's original notice where after the Parties shall in good faith endeavour to settle the situation. In the event that the controller's reasonable concerns still remain after conclusion of such good faith effort, then the controller shall, as its sole remedy, have the right to terminate the Agreement forthwith by written notice without liability for either Party.

Annex III – Technical and organisational measures

Information Security Approach

An ISMS based on ISO/IEC 27001 using a continual improvement model is used to enhance information security over the time it is operated on an ongoing basis. To measure success testing, monitoring, and measuring effectiveness of controls is carried out internally as part of ISMS management and externally as part of yearly auditing.

Continual, systematic risk assessment considers threats, vulnerabilities and impacts affecting confidentiality, availability and integrity of assets and devises treatment plans based on risk scoring to address risks that are not acceptable via technical and organisational controls.

Responsibility and therefore accountability is assigned to policies, procedures and controls designed to meet organisational and customer information security requirements.

Business Continuity

A business continuity policy backed by procedures is maintained, aimed at mitigating disaster scenarios that may impact operations targeting various situations, including:

- Loss of facilities (e.g., via a pandemic, estate issues, natural disaster etc.)
- Impairment of facilities (e.g., loss of supporting utilities, internet connectivity, etc.)
- Loss or corruption of information assets including production systems data.

The policy and procedures detail requirements (RTO, RPO etc) and resolutions for each scenario and mitigating controls (e.g., defining a backup regime and requirements for periodic backup testing) so that normal operations may resume as rapidly as possible.

Data Protection Controls

Baseline configuration and ongoing management of employee devices is carried out via MDM, and servers using infrastructure-as-code, including installation of security software relevant to the platform in question which may include EDR/Antivirus and/or intrusion detection software.

Cryptography policies cover requirements such as strong, unbroken encryption ciphers or hashing algorithms and key management. Data at rest (including documents in object storage, databases, employee devices, backups etc.) and transport over public networks is encrypted.

Identity and Access Management systems are integrated with internal systems where possible, with a requirement for auditable management of access rights assignment and operated using the principle of minimum-privilege and role-based access.

Log management is centralised and heavily restricted to allow troubleshooting and performance & security monitoring of systems. Where systems do not support centralised logging, secure log shipping measures are utilised to enable this.

Passwords are governed by a password policy defining requirements such as complexity, multi-factor authentication and usage of an enterprise password management utility.

Retention controls are applied to different systems containing applicable data governed by a retention policy designed by our Legal Department and DPO to meet legal and regulatory requirements.

Supplier management procedures govern the onboarding and ongoing relationship with third party suppliers, considering legal, physical, and technical security controls utilised in the delivery of services at locations where data is processed.

Data minimisation and quality

Scrive does not require or retain any personal data that is not needed for a signing process to be completed and/or such data that the customer has defined to be a part of their signing process(es), and then only until the customer deletes the signing process from the system.

Regardless of input method, input data is escaped to avoid injection attacks. The controller may, if so desired and when feasible, define the format of permitted input by means of regular expressions on a case-by-case basis. Input of data of known format (e.g. personal identification numbers) is validated automatically by the Scrive Services used.

Data portability

Scrive Services that feature document export offer the output of documents in ISO 32000 PDF format and of metadata in JSON and/or CSV format.

Other transactional data can be exported in JSON format for the duration of the retention period for transaction history of the relevant service.

Data erasure

Scrive will retain personal data within the Services in accordance with the processing operations for data retention as set forth for the relevant Scrive Services as subscribed to by the controller. When a transaction is deleted from the Scrive Services, Scrive will retain internal transaction identifiers (which cannot be used to identify any individual) and the date and time of that transaction, for billing and statistics purposes. Data that has been captured by the daily backups will, in accordance with the processor's data retention policy, be retained in AES-256 encrypted format until it is automatically deleted after a period defined in said policy (i.e. no longer than six months).

- - -