Version: 4.0 of April 20, 2018

Changes compared to the version 'V3.0' are highlighted in yellow on pages 12 and 14.

Data Processing Terms for Cloud Services[1]

The Customer (hereafter defined) is agreeing to these Data Processing Terms, including the attached schedules (collectively, the "DPT"), because it has entered into a certain Service Agreement (hereafter defined) with the Company (hereafter defined). These DPT are entered into by Customer and Company as of the effective date of the Service Agreement. In case the Service Agreement has been entered prior to the effective date set forth above and the Service Agreement is subject to an extension of its term, these DPT supersede any data processing terms previously entered into by Customer and Company.

These DPT are always incorporated into each Service Agreement by reference. In case of conflict or discrepancies between the terms of the Service Agreement and the DPT, the terms of the DPT shall always prevail and control. The Customer is advised to read them. In the event Customer disagrees with certain of these terms, Customer is invited to provide remarks and comments prior to the signature of the Service Agreement. In case Company and Customer agree to amend the DPT the agreed upon amendment will be appended to the Service Agreement.

1- The reason for the DPT

The Solution (hereafter defined), that is software based or a combination of software and hardware, allows the processing of Customer Personal Data (hereafter defined) to direct the benefit of the Solution (hereafter defined) to the Customer as well as in the case of a Customer Offer (hereafter defined) to End-Users (hereafter defined).

The Solution may be hosted in Hosting Entity (hereafter defined) that is not controlled by Company. Section 4 below set forth a detailed explanation of the role of Hosting Entity (hereafter defined).

Customer and Company acknowledge and agree that Data Privacy Laws (hereafter defined) may apply to the processing of Customer Personal Data. In such a case the DPT is applicable.

2- Definitions

Notwithstanding any contrary definitions in the Service Agreement, capitalized terms used in these DPT whether in singular or in plural, shall have the following meanings in the context of this DPT:

Applicable Data Protection Law: means Data Privacy Laws applicable to Customer as the Data Controller of the Personal Data.

Authorized Employees: means employees of the Gemalto Group who have a need to know or otherwise access Customer Personal Data to enable the performance of the Service Agreement.

Authorized Persons: means (i) Authorized Employees; and (ii) Sub-processor who have a need to know or otherwise access Customer Personal Data to enable the performance of the Service Agreement.

Breach of Security: means the unauthorized acquisition or unauthorized use of either (i) unencrypted data or (ii) encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person, which creates a substantial risk of identity theft or fraud against an individual.

Company: means the legal entity member of the Gemalto Group entering into the Service Agreement.

Customer: means the legal entity entering into the Service Agreement.

[1] Cloud Services delivery model: delivered as a Service outside customer's premises.

Customer Personal Data: means the Personal Data contained in the data directly transmitted by the Customer, or on its behalf, or by End-Users, into the Solution.

Customer Offer: means the services offered by Customer to End-Users.

Data Center: means premises property of the Gemalto Group where the Solution is installed.

Data Controller: means the natural or legal person who determines the purpose and the means of the processing of Personal Data.

Data Privacy Laws: means all laws, rules, regulations, governmental requirements, codes as well as international, federal, state, provincial laws applicable to Personal Data.

EU Model Contract: means the standard contractual clauses (processors) for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection.

End-Users: means natural person or legal entity that accepts to receive the Customer Offer.

GDPR: means the General Data Protection Regulation (2016/679) of the European Parliament and the Council 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.

Gemalto Group: means collectively or individually legal entity(ies) controlled by Gemalto N.V. a company organized under the laws of Netherlands. In this context control means direct or indirect (through any number of successive tiers) ownership of: (a) more than fifty percent (50%) of the outstanding shares having the right to vote for the election of directors or other managing authority of the subject entity; or (b) in the case of an entity which does not have outstanding shares (e.g., a partnership, joint venture or unincorporated association), more than fifty percent (50%) of the ownership interests having the right to make decisions for the subject entity.

Hosting Entity: means a legal entity, that is not signatory of the Service Agreement, and that has entered into an outsourcing agreement with System Administrator to host the Solution. The hosting entity could be a public cloud service provider.

Legal Process: means a data disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.

Personal Data: **:** means (i) data which relate to a living individual (whether in personal or family life, business or profession) who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, as well as (ii) information that can be utilized to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, etc. This definition may be adapted with respect to the Applicable Data Protection Law (for example some Privacy Laws cover not only individual but also legal entities, and not only living individuals but deceased individuals).

Rights of Individuals: means the legal rights of individuals to access, rectify, delete, and port Personal Data.

Security Program: means the security program attached as **Schedule 1** of this DPT which is solely applicable to management, operational and technical control under the full control of Company.

Service Agreement: means that certain agreement entered into between Customer and Company.

Solution: means the information system used for storing, managing, using and gathering of Customer Personal Data.

Specific Services: means, outside the scope of tasks of the System Administrator, certain services set forth in the Service Agreement such as the provision of aggregate analytic and statistical report.

Sub-processor: means legal entities engaged to provide Specific Services that may require certain processing of Customer Personal Data.

S**ystem Administrator:** means a legal entity member of the Gemalto Group who is responsible for the upkeep, configuration, and reliable operation of the Solution, such as the installation, upgrading computer components and software, providing routine automation, maintaining security policies.

Third Party Claim: means a demand or assertion by a third party seeking, as a matter of right, payment of money, or other relief.

3- **Data Controller and Data Processor**

3.1 Customer is the Data Controller of the Customer Personal Data, and Company, via its engagement of Sub-processors, is the processor of Customer Personal Data. Furthermore, the System Administrator via the engagement of the Hosting Entity or via the Data Center, could be processing Customer Personal Data at least with respect of enabling Customer to store the Customer Personal Data into the Solution.

3.2 In certain cases Customer is directly connected to the Solution, thus Customer is directly performing, or allowing End-Users to undertake, the provisioning of the Solution with Customer Personal Data.

3.3 Neither Company, Sub-processors, System Administrator nor Hosting Company have collected the Customer Personal Data. Sub-Processors and System Administrator processes Customer Personal Data as data processor at the direction and with prior approval of Customer in accordance with the terms of the Service Agreement.

4- **Transparency Requirements**

4.1 Prior to entering into the Service Agreement with Customer, Company will deliver to Customer a document called "Processing Form" a template of which is attached as **Schedule 2** to the DPT. This document describes the type of Customer Personal Data to be processed by the Solution, the name and location of the Hosting Entity or the Data Center where the Solution is Hosted, the System Administrator and the Sub-processors involved in the Processing of the Customer Personal Data, how the Customer Personal Data is processed, the flows of the Customer Personal Data, and the period of time the Customer Personal Data is retained during the term of the Service Agreement after the expiry or termination of the Service Agreement.

4.2 Once agreed upon the Processing Form is appended to and made part of the Service Agreement.

5- **Instructions by Customer**

5.1 Customer Personal Data can only be processed within the scope of the Customer's instructions. The Service Agreement set forth the instructions of the Customer regarding the type, extent and method of Processing of the Customer Personal Data taking into account the specifications of the Solution subject matter of the Service Agreement and the content of the Processing Form (referred in Section 4 above). Except as set forth in this DPT, neither Company, Sub-processors, System Administrator nor Hosting Company will review, share, distribute, nor reference any Customer Personal Data.

5.2 Any change in the processing of the Personal Data during the term of the Service Agreement can only occur with the prior written approval of the Customer.

6- **Hosting Entity and Data Center**

6.1 As of the applicable data of the DPT, the Processing Form (as referred in Section 4 above) identifies each Hosting Entity that has entered, directly or indirectly, into a specific hosting agreement with each relevant System Administrator.

6.2 Customer uses the Solution hosted on the system of Hosting Entity or the Data Center to transmit or process Customer Personal Data. It has to be understood that Hosting Entity and Data Center do not determine or have knowledge of the types of data stored by Customer and/or how that data is accessed, exchanged, processed or the classification of that data.

7- **Sub-processors**

7.1 Depending on the provisioning to Customer of Specific Services, Company may engage Sub-processor to provide in whole or in part the Specific Services.

7.2 In the event statistics associated with an aggregate report, and/or specific report services for billing purpose are offered as part of the Specific Service, the delivering of such Specific Services requires the use of a software program that (i) accesses the production database of the Solution in a secure manner and (ii) extracts certain data to store it in a data warehouse located in a Gemalto Group's premises where the data is analyzed to build, in aggregate format, the agreed upon dashboards and reports. If such statistics and reporting services is offered as part of the Service Agreement it will be specified in the Processing Form set forth in section 4 above also indicating where the data warehouse is located as well as the identification of the Sub-processor.

7.3 Except with respect to Section 7.2 above, the involvement of Sub-processor requires the prior written consent of the Customer, which is given as part of the signature of the Service Agreement.

7.4 Where the Sub-processor is located in a non-adequate country (a country that is deemed not to provide an adequate level of protection for Personal Data within the meaning of EU Directive 95/46/EC or the GDPR), Company shall procure that the Sub-processor enters into an EU Model Contract. Note that this section is based on EU data privacy laws. Thus, it may not apply in certain jurisdictions.

7.5 Except with respect to Section 7.2 above, in the event Company and Customer have already entered into a Service Agreement and Company is envisaging to engage a new Sub-processor, Company will inform Customer with detailed information on the Sub-processor and the portion of the Service Agreement to be sub-contracted, and request Customer written consent via an amendment to the Service Agreement. If Customer objects to the engagement of the new Sub-processor it shall immediately inform Company in writing. Immediately following receipt of the objection Customer and Company shall decide on an alternative solution.

8- **Transmission of Personal Data to other countries**

8.1 As indicated in Section 4 above, the Solution is hosted at the Hosted Entity or the Data Center. In the event the use of the Solution by Customer triggers a cross-border transfer of Customer Personal Data, the Customer understands that such cross-border transfer of Customer Personal Data may be subject to specific requirements imposed by the applicable Data Privacy Laws with the burden of such specific requirements being carried by the Data Controller.

8.2 In the event such cross-border transfer of Customer Personal Data could require the entering into a specific cross-border transfer agreement in light of the Applicable Data Protection Law. The Company and Customer will collaborate in order to satisfy this requirement.

9- **Customer Commitments**

9.1 Customer represents and warrants that the Customer Personal Data it provides for Processing can be processed lawfully (e.g., lawful collection, compliance with obligation to inform and compliance with the applicable Data Privacy Law).

9.2 Customer shall not by any of its act or omission put Company, System Administrator, Sub-processor, Hosting Entity and Data Center in breach of any Data Privacy Laws in connection with the processing of the Customer Personal Data.

9.3 It is the responsibility of Customer to assure that the Personal Data processed is accurate, adequate and complete.

10- **Security Principles**

10.1 In accordance and within the limit of the Security Program the Gemalto Group implements technical and organizational measures to protect Customer Personal Data against Breach of Security. Customer agrees that it is solely responsible for its use of the Solution for processing the Customer Personal Data, including its account authentication credentials, and that Company, System Administrator, Sub-processor, Hosting Entity and Data Center have no obligation to protect Customer Personal Data that Customer elects to store or transfer outside, Sub-processor, Hosting Entity and Data Center. In particular Customer when providing Personal Data to the Solution may be subject to security rules recommended by Company and set forth in **Schedule 2** of the DPT. The Customer solely assumes all risks, liabilities and consequences if it fails to abide to such security rules.

10.2 Company will take appropriate steps to ensure compliance with the Security Program by the System Administrator, Sub-processor, Hosting Entity and Data Center, to the extent applicable to their scope of performance. It means that the Security Program does not cover the security offered by the public cloud service provider acting as Hosting Entity. Customer has to consider the security of the public cloud service provider, acting as Hosting Entity, in evaluating the overall security protecting the Personal Data.

10.3 (a) If Company becomes aware of a Breach of Security it will promptly notify Customer of the Breach of Security, and take reasonable steps to minimize harm and secure Customer Personal Data. Notification(s) of a Breach of Security will be delivered via the notification contact provided by Customer in the Service Agreement or, at Company's discretion, by direct Customer communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring that the contact information set forth above is current and valid, and for fulfilling any third party notification obligations. Company obligation to report or respond to a Breach of Security under this Section 10.3 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Breach of Security.

(b) Promptly following Company's notification to Customer of a Breach of Security, Customer and Company shall coordinate with each other to investigate the Breach of Security. Company leads the investigation and agrees to reasonably cooperate with Customer in the handling of the Breach of Security, including, without limitation: (i) assisting with any investigation; (ii) providing Customer with physical access to the facilities and operations affected which are under the control of the Gemalto Group; (iii) facilitating interviews with Authorized Persons; and (iv) making available the relevant records, logs, files, data reporting and other materials, concerning the Customer, required to comply with Applicable Data Protection Law, regulation, or as otherwise reasonably required by Customer.

10.4 Notwithstanding anything to the contrary in the Service Agreement or the Security Program, Company, Sub-processor, System Administrator, Hosting Entity and Data Center obligations extend only to those systems, networks, network devices, facilities and components over which they exercise control. The Security Program does not apply to: (i) Customer Personal Data shared with either of Company, Sub-

processor, System Administrator, Hosting Entity and Data Center, that is not data stored in the Solution; (ii) Customer Personal Data in Customer's virtual private network (VPN) or a third party network, or (iii) Customer Personal Data processed by Customer or its users in violation of the Service Agreement or the Security Program.

10.5 Request to audit the Security Program shall be sent by Customer to the Company via the contact notification set forth in the Service Agreement. In particular, Company (via its Corporate Security Department) and Customer will discuss and agree in advance of the identity of a suitably qualified and independent third party auditor to carry the audit, and the reasonable start date (i.e., at a minimum thirty (30) calendar days from the date of receipt by Company of the request to audit), scope and duration of and security and confidentiality controls applicable to any such audit. Customer is made aware that the audit of the Security Program shall take into account the security rules and policies of each Hosting Entity, the Data Center, Sub-processor, that can impose some limits on the expected scope of the audit by Customer. Company (via its Corporate Security Department) is available to provide details on such limits, if any. Company is not responsible for any costs incurred by Customer as well as fees charged by any third party auditor appointed by Customer in connection with an audit. Furthermore, Company reserves the right to charge fees and costs for any request for audit that exceeds one (1) per calendar year.

10.6 Customer Personal Data are subject to certain confidentiality obligations set forth by the Security Program. Consequently, a Breach of Security exposing Customer Personal Data shall not trigger the confidentiality provision set forth in the Service Agreement covering data and information that are deemed confidential information. This section 10.6 shall govern and prevail in case of conflict with the confidentiality provision set forth in the Service Agreement.

11- **Cooperation regarding requests and inquiries**

11.1 Company will promptly (and in any event no later than five (5) calendar days after receiving a complaint, request or inquiry) inform Customer of any complaints, requests or inquiries received from individuals, including but not limited to requests to correct, delete or block Customer Personal Data. Company does not respond to the individual directly unless specifically instructed by Customer save where Company or Sub-processor, Data Center, Hosting Entity, or System Administrator is required by law, or Legal Process, to respond, in which case it shall respond within a reasonable period of time, and in any case as required by the applicable law. Company will cooperate with Customer to address and resolve any such complaints, requests or inquiries.

11.2 Company will deal promptly and appropriately with enquiries of Customer related to the Processing of Personal Data under the Service Agreement. Company will cooperate with Customer where this is necessary for the performance of Customer's privacy impact assessments.

11.3 Any request made by Customer that is triggered by the application of the Rights of Individuals shall be made by Customer to Gemalto either (a) as per the terms of the notification provision set forth in the Service Agreement or (b) in the event Customer purchases technical support, as per the terms of Section 5.2 of Schedule 3 of the DPT, and shall contain the following information:

- the identification of the Service Agreement;
- the identification of the Personal Data in question;
- specify the Solution where the Personal Data is likely stored.

12- **Confidentiality, Archiving and Destruction of Persona Data**

12.1 Company or Sub-processor, Data Center, Hosting Entity, or System Administrator, shall not Disclose Customer Personal Data in any way to any third party without the prior written approval of the Customer, except where, (i) the disclosure is necessary for the performance of the Service Agreement, or (ii) where, in accordance with Section 10 above, Customer Personal Data needs to be disclosed to a competent public authority to comply with a Legal Process.

12.2 As a general principle Company or Sub-processor, Data Center, Hosting Entity, or System Administrator, in accordance with the requirements of applicable laws, do not keep Customer Personal Data longer than necessary than the purpose for which the Customer Personal Data were entrusted by Customer to Company as per the Service Agreement, or, as applicable, within the limit of the PCI-DSS, PCI-CP standards, or the VISA, MASTERCARD requirements, or any other payment network operators.

12.3 Following the implementation of Section 12.2 above, the Personal Data is deleted irretrievably.

12.4 In the event Customer requires that the Customer Personal Data be archived Company and Customer will have to enter into an archiving agreement including, but not limited to, the following provisions:

a) Duration of the archiving;
b) Type of storage;
c) Location;
d) Access conditions;
e) Pricing conditions.

13- **Support Service**

13.1 The terms and conditions covering the technical support service are set forth in **Schedule 3** attached to this DPT.

14- **Indemnification and Liability**

14.1 Subject to Section 14.2 below, Company shall defend, and indemnify Customer, from and against any and all losses, damages, liabilities, actions, judgments, interest, awards, penalties, fines, costs or expenses, including reasonable attorneys' fees ("Losses"), directly arising out of or directly resulting from a Third Party Claim against Customer arising out of or resulting from a Breach of Security affecting the Customer Personal Data provided that it is established that the terms of the Security Program has been breached in whole or in part or the Breach of Security is caused by a defect in the implementation of the Security Program.

14.2 The foregoing indemnification is conditioned on Customer: (a) notifying Company promptly in writing of a Third Party Claim; (b) giving Company sole control of the defense thereof and any related settlement negotiations; provided, however, the Company shall have no authority to enter into any settlement or compromise on behalf of the Customer without the prior consent of Customer which shall not be unreasonably withheld or delayed. If Company does not undertake the defense of a Third Party Claim, the Customer shall have the right to conduct the defense of the Third Party Claim at its sole defense, provided (i) nothing in the foregoing shall limit or be deemed to limit a party's right to dispute that a Third Party Claim (and/or any Losses arising therefrom) relates to a Breach of Security, and (ii) if Company has agreed that a Third Party Claim relates to a Breach of Security, the Customer shall have no authority to enter into any settlement or compromise on behalf of Company without Company's consent (which consent shall not be unreasonably withheld or delayed). In all circumstances, the Customer shall have the right to participate in the defense of any proceedings with counsel of its own choosing, at its sole expense, and shall cooperate with Company in the defense of a Third Party Claim maintained thereby.

15- **Changes**

15.1 If Company:

a) determines that it, or a Sub-processor, Data Center, Hosting Entity, or System Administrator, is unable at any time and for any reason to comply with the obligations set forth in this DPT and cannot cure this inability to comply; or

b) becomes aware of any circumstance or change in the applicable Data Privacy Law, that is likely to have a substantial adverse effect on the Company, or Sub-processor, Data Center, Hosting Entity, or System Administrator, ability to meet the obligations set forth in this DPT:

Company will promptly notify the Customer thereof, in which case the Customer will have the right to temporarily suspend the processing of the Customer Personal Data until such time the processing is adjusted in such a manner that the non-compliance is remedied.

16- **Evolution of the DPT**

16.1 At the request of Customer, Company and Customer shall from time to time evaluate the processing of Customer Personal Data. If Customer considers that changes are required in the processing of Customer Personal Data in order to comply with Applicable Data Privacy Law, Customer and Company shall collaborate to evaluate the changes to be made. Company will inform Customer of any circumstances which may be relevant in this respect, including, but not limited to:

1) material changes in the provision of the Service Agreement; or
2) merger, reorganization, sale of all or substantially all of the assets, change of control or operation of law affecting Company, Sub-processor, Data Center, Hosting Entity, or System Administrator.

Schedule 1: Security Program

Main Principles of Gemalto Group's Security Program

Preface:

This document sets out the main elements of the Gemalto Group's security program dedicated to the safeguarding of the data entrusted to us.

In the event of any questions or the request of deeper details, customers are invited to contact its Gemalto representative who will then involve the Gemalto Group "Corporate Security department" as needed.

Principles:

This Security Program aims at ensuring that in the current context of our international activities.

Our security program aims at:

a) identifying through risk analysis, potential threats to Customer information;
b) implementing security solutions (both processes and tools) to limit risks to our systems;
c) training our employees and third-party service providers to implement the Security Program;
d) Monitoring the security of our systems and processes;
e) providing clear information on the processing of Customer information;
f) responding to customers queries and request on the protection of their information;
g) preparing ourselves in case of crisis

The following paragraphs describe in more details the main principles of the Security Program protecting Customer information.

A- Main Principles

Our security program governance is:

- Based on the several policies applicable to the Gemalto Group as well as to all Gemalto Group employees, employees of third-party services providers and external people servicing or dealing with the Information System (as hereafter defined).

- Under the responsibility of the Corporate security Department and IT department and locally under the management of designated security and IT manager. And supported by security councils that operate in accordance with the ISO27001 standard.

- Periodically reviewed and its application is checked during local and central security audits. Furthermore, technical security audits are undertaken at corporate and local level. The periodicities of such audits vary in light of the security level, sensitivity and vulnerability of the system.

Our security program concentrates on the following elements:

Personal Information Identification and Classification: The purpose of the personal information identification and classification policy is to establish a system of priorities for protecting information and assets, in order to ensure that protection levels are commensurate with the value of the information or system being protected throughout their lifecycle, from elaboration to destruction. The use of classification levels allows the organization to focus protection costs on information of the highest value. This policy covers the following main elements:

- Establish Gemalto Group corporate rules for the management of information, in respect with its sensitivity;
- Confidentiality dimension of information through a labelling scheme with five classification levels from Secret (highest) to Public (lowest);
- Protection of the area where information is located is in adequacy with the information classification level;
- Restricted logical access to computers and networks follow the same rules as physical access restrictions;
- Recording of the reception of physical media containing confidential information;
- Rules for the transmission of information;
- Rules for physical, electronic and media storage;
- Rules for destruction;
- Clean desk policy rule.

Physical and Environmental Security Policy: Setting the primary means of defense against theft or misuse of products and services supplied by Gemalto Group and are required to protect our know-how. They are also a protection for our personnel. This policy covers the following main elements:

- Applicable to all Gemalto Group sites. A site is a physical location where Gemalto Group employees are based or where Gemalto operations are conducted;
- Each Gemalto Group site must comply with defined minimal security features in accordance with their domains of activity and the identified risks of their processes;
- Each Gemalto Group site is subject to regular audit performed by the Corporate Security Team to verify compliance with the policy;
- Each Gemalto Group site has a security manager;
- Each Gemalto Group site is organized in three zone levels classified according to the security services they offer.

Configuration Management System Security Policy: Designed to establish Gemalto Group corporate security rules for the management of software during their development and when they are delivered. This policy covers the following main elements:

- Major security topics: confidentiality, integrity, availability, accountability and traceability;
- Software management through an IT tool called a Configuration Management System (CMS);
- Applicability to all Gemalto employees, consultants, or contractors working within Gemalto facilities or connected via networks or remote access;
- Implementation of this policy is checked during local and central security audits;

- Roles and responsibilities in the application of this policy is allocated to a wide number of Gemalto's employees, comprised of security personal and personal involved in the development and management of software;
- Rules setting restricted access to the room where sensitive software is stored;
- Rules addressing the use of encryption to assure confidentiality.

Security Assurance Plan for Software development: In order to provide an end to end consistent security and to fulfill the time to market constraints, we define "Targets of Trust". This notion qualifies the overall risk exposure according to the project context. Based on this target, various security activities are performed during the software development. Thus, the security activities put in place are driven by the risks we face.

This trust qualification can be done with the Customer in order to highlight the main risks drivers.

Activities performed during software development are:

- **Education program** dedicated to dev teams
- **Baseline requirements**: foundation requirements providing a "by default" protection level inside the software. Based on Risk Assessment, additional countermeasures are implemented on top of these foundation requirements.
- **Risk management**: identification, ranking and treatment of the main risks driven by the use cases and the supporting software.
- **Code review**: controls performed on the source code (common weaknesses identification and fix)
- **Vulnerability assessment**: performed during and after the development. It provides a classification of vulnerabilities and lead to containment and corrective actions.
- **Security testing**: ensures each security requirement is implemented and provides the expected protection level (test plan coverage, dynamic application testing, penetration testing).

Security Rules for Sub-contracting Software development: In addition to the Configuration Management System Security Policy, Gemalto Group has designed a policy addressing the acquisition of third parties software development services. This policy aims at assuring the confidentiality of the information provided to the service provider. This policy covers the following main elements:

- Defining three security levels establishing a level of risk in light of the software security sensitivity. Development of software with the highest level of security sensitivity (level 3) cannot be outsourced;
- Authorized outsourcing of software is subject to a contract imposing the application of ISO 27001 standard and security audit;
- Access to Gemalto Group's network is subject to a risk assessment that is used to define the required point of control, security acceptance criteria and the assignment of a security representative;
- Validation by Gemalto Group security personnel of the service provider's physical and logical configurations;
- The information made available to the service provider is previously classified by Gemalto in accordance with the personal information identification and classification policy. Based on such classification the service provider is bound to implement the applicable Gemalto Group's rules;
- Employees of the service provider are subject to security screening to obtain access to information. Only a minimum number of employees can have access to the information and they have to be educated on the applicable level of security.

Information System ("IS") Security Policy: Designed in accordance with ISO27001 standard to (a) enlighten the IS security principles are valuable for key strategic elements, such as the stakes, the referential, the

business security needs and miscellaneous threats and (b) ensure that our security requirements are in accordance with our customers' requirements. This policy covers the following main elements:

- Specification of the roles and responsibilities of Gemalto Group's employees involved in the system security;
- Applicable to all Gemalto Group's sites, Gemalto Group's employees, and service providers working on the Gemalto Group's IS;
- Mandatory review of this policy every two years;
- Define security levels to determine the applicable security zoning all over the Gemalto sites;
- The security zoning defines applicable security rules depending on the sensitivity of the information processed;
- Define the roles and responsibilities of the Gemalto Group's personnel in charge of assuring the implementation of this policy;
- Risk assessment process;
- Compliance with legal and regulatory requirements in jurisdictions where Gemalto Group is conducting its business;
- Security rules applicable to the use of mobile equipment (e.g.., laptop, tablet, mobile phone);
- Dedicated access control depending on the level of security classification;
- Rules to be followed by all persons granted access to the IS, including third party service providers to assure that the same level of security is implemented;
- Auditing principles defining the applicable audit process depending on the applicable level of security;
- Third party penetration testing is put in place with third party providers;
- IS security controls through the use of firewalls, intrusion detection, prevention systems and the use of intranet and internet proxies to protect IS from outside attack;
- Protection against malicious code through anti-virus software, virus detection;
- Real time monitoring to address any outside attack to our IS;
- Vulnerability survey of our IS that could trigger deployment of security patches;
- Pursuant to agreed upon contractual terms, implementation at Gemalto's sites of disaster recovery plan to assure the availability of the IS.

B- Computer Security Incident Response Team (CSIRT) and Security Training program

Gemalto Group has set-up a centralized organization to reinforce the prevention and protection against Cyber security risks. This organization operates according to RFC2350 which specifies the expectations for Computer Security Incident Response and is supported by LEXSI, a commercial CERT.

The Gemalto CSIRT is built of several experts in Cyber defense and incident response, encompassing forensics, network investigations and penetration testing. Most of our experts are certified: GIAC Forensics, EC-Couciel (CEH) depending on their scope of responsibilities.

Every user of the IS has to be trained in information security practices relevant to their use of Gemalto information and systems. Testing of user knowledge is tracked.

Human Resources department is responsible for orientation of all new employees in basic information security principles. Direct managers are responsible for informing each employee, through awareness programs, about information security policy, standards and procedures. IT managers are responsible for job specific technical training of IT team. Security department is responsible for training, certification and tracking of information security practices.

Schedule 2: Data Processing Form

This schedule provides description of the service provided by the legal entities listed in this document and acting as Data Processor, the types of data to be processed and the purposes for which the data is being processed, and describes the purpose duration, mandatory retention requirements (if any).

Description of the Services:

[TO BE COMPLETED WITH THE TYPE OF SERVICE TO BE DELIVERED]

Client(s) is/are:

[TO BE COMPLETED WITH THE NAME OF THE CLIENT(S)]

Personal Data Processing:

[TO BE COMPLETED WITH A DESCRIPTION OF THE PROCESSING UNDERTAKEN BY EACH COMPANY]

Breakdown of data: [TABLE TO BE COMPLETED]

	Data type	Purpose	Data retention period
1.			
2.			
3.			
4.			
5.			

Location of the Hosting Entity or Data Center and identification of the System Administrator:

[TO BE COMPLETED WITH THE LOCATION OF THE PROCESSING EQUIPMENT INCLUDING THE LOCATION OF THE PROCESSING EQUIPMENT USED TO GENERATE STATISCAL RESULT]

(If applicable) Name and location of the Sub-processor providing reporting services for statistical and billing purpose.

[TO BE COMPLETED WITH THE LOCATION OF THE TEAM PROVIDING REPORTING SERVICES FOR STATISTICAL AND BILLING PURPOSE.]

Transfer of the personal data:

To protect the Personal Data Gemalto makes the following security recommendations any exceptions to these security recommendations has to be recorded in Section II below:

I- Security Recommandations

A/ **Exchange protocol**: is in charge to protect Personal Data during their transit from and to customer premises to and from the Hosting Entity or the Data Center. The main objective of exchange protocol is to ensure the authentication of the parties and the integrity of the transfer.

- Recommendation: Gemalto Allynis Connect solution using secured protocols (no email).

B/ **File Encryption**: is used to protect the Personal Data during their transit from Allynis Connect platform to the Solution. Recommended file encryption is based on OpenPGP standards. On top of the PGP file encryption the Personal Data files are transiting in a secure tunnel.

- Recommendation: PGP encryption with:
  - AES - 128 bits or higher for symmetric part configuration
  - RSA ≥ 3072 bits for asymmetric part configuration (key transportation)

Note: Asymmetric RSA ≥ 2048 bits and symmetric 3DES-112 bits or 3DES-168 bits are however tolerated when used with mid-term cryptographic periods.

For the implementation of the encryption it is recommended to follow NIST800-57 Part 1.

C/ **Record Encryption**: in case record encryption is available as specified by Gemalto on a case-by-case basis, it is needed to protect data until it reaches a secure safe (database or the HSM of the customer application).

- Recommandation: AES - 128 bits or higher

Note: symmetric 3DES-112 bits or 3DES-168 bits are however tolerated when used with mid-term cryptographic periods.

For the implementation of the encryption it is recommended to follow NIST800-57 Part 1.

II- Exceptions to the Security Recommendations

[*TO BE COMPLETED IF REQUIRED*]

Schedule 3: Data Processing Terms for Technical Support Services

1. Certain definitions

As used herein,

Client Information: means personal information collected directly from Customer's employees or agents via the Portal or Support HotLine.

Customer: means the legal entity that purchases Support Service from the Gemalto Group.

Gemalto: means Gemalto SA a company organized under the law of France located at 6 rue de la Verrerie Meudon 92190 (France), acting on its own behalf and on behalf of each company of the Gemalto Group.

Gemalto Group: means collectively or individually legal entity(ies) controlled by Gemalto N.V. a company organized under the laws of Netherlands. In this context control means direct or indirect (through any number of successive tiers) ownership of: (a) more than fifty percent (50%) of the outstanding shares having the right to vote for the election of directors or other managing authority of the subject entity; or (b) in the case of an entity which does not have outstanding shares (e.g., a partnership, joint venture or unincorporated association), more than fifty percent (50%) of the ownership interests having the right to make decisions for the subject entity.

Log Files: means files that record trails sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results and that may contain data such as IP address, MSISDN, EID, IMSI, user name.

Personal Data: means any information relating to an identified or identifiable individual where the individual is associated with Customer.

Portal: means the web portal made available by Gemalto to make a request for Support Service. The web portal requires registration to access it and the completion of a form to make a request for support, each case triggering the disclosure of certain Personal Data such as full name and professional e-mail address.

Processor: means legal entities member of the Gemalto Group.

Solution: means the information system managed by the Gemalto Group which is used to process data provided by Customer.

Support Hotline: means a telephone number available to make a request for Support Service and that requires the disclosure of Personal Data for the completion of the request such as full name and professional e-mail address.

Support Service: means the provision by Gemalto and companies of the Gemalto Group of technical support contractually agreed upon with Customer.

2. Purpose of Processing of Data

2.1 The Solution is generating Log Files whose content has been designed to record only the data necessary to the Support Service, and that are used for the purpose of providing the Support Service.

2.2 Gemalto is collecting Client Information for the purpose of providing the Support Service.

2.3 Gemalto determines the purpose and means of the processing of the Log Files and Client Information, hence Gemalto is the entity controlling the Log Files and Client Information.

3. Quantity of Data

3.1 Gemalto restricts the processing of Log Files and Client Information to the data that is reasonably adequate and relevant for the purpose of the Support Service.

3.2 Gemalto retains the Log Files and Client Information for the duration of the Support Service, to the extent reasonably necessary to comply with an applicable legal requirement or advisable in light of an applicable statute of limitations.

3.3 Promptly after the applicable retention period has ended, the Log Files and Client Information are securely deleted or destroyed.

4. Information and Consent of Individual

4.1 With respect to the Client Information:

a) a privacy notice is made available to individuals via the Portal, and
b) collected via the Support Hot Line, it belongs to Customer to inform its employees or agents of these Data Processing Terms for Support Service.

4.2 Employees or agents of Customer consents to the processing of the Client Information at the time of entering into the Portal and when answering to the questions raised by the Support Hot Line.

5. Rights of individuals

5.1 Customer and employees and agents of Customer (hereafter collectively or individually referred to as the "Interested Party") have the right to request an overview of the data processed for the purpose of the Support Service. If the data is incorrect or incomplete, the Interested Party has the right to have the data rectified, deleted or blocked.

5.2 To undertake the rights set forth in Section 5.1 above the Interested Party has to make a request for support via the Portal. The request shall contain the following information:

- specify the type of data in question;
- specify, to the extent reasonably possible, the data system in which the data likely is stored
- specify the circumstances in which Gemalto obtained the data;
- for employees or agents of Customer, confirm the employment or agency relationship with Customer.

5.3 Within four (4) weeks of Gemalto receiving the request or the objection, Gemalto shall inform the Interested Party in writing of Gemalto position with regard to the request or the objection and any action Gemalto has taken or will take in response.

6. Security

6.1 Gemalto takes appropriate commercially reasonable technical, physical and organizational measures to protect the Log Files and Client Information from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

6.2 Staff is provided access to Log Files and Client Information only to the extent necessary to perform the Support Service and to perform their job.

6.3 Staff in contact with Log Files and Client Information shall meet their confidentiality obligations as specified by contract, and Gemalto's policies.

7. Cross-Border Transfer

7.1 Gemalto permits remote access to the Log Files and Client Information to Processors located in different countries of the world.

7.2 Processors are only allowed to process Log Files and Client Information if it has entered into a written contract with Gemalto that includes the following provisions:

a) the Processor can only process the Log Files and Client Information only in accordance with Gemalto's instructions and for the purpose of the Support Service;
b) the Processor shall keep the Log Files and Client Information confidential;
c) the Processor shall take appropriate technical, physical and organizational security measures to protect the Log Files and Client Information; and
d) the Processor shall not permit further processing of the Log Files and Client Information without the prior written consent of Gemalto.

7.3 The transfer of Log Files and Client Information to a Processor located in a country that is not considered to provide an 'adequate level of protection for Personal Data' is only permitted by Gemalto only if the Processor has entered with Gemalto into a contract that conforms to any model contract required under applicable Personal Data protection law or regulation (if any).

8. Policies and Procedures

8.1 Gemalto develops and implements policies and procedures to comply with these Data Processing Terms for Support Service.

8. 2 Gemalto maintains readily available information regarding the structure and functioning of the Support Service.

9. Applicable Privacy Law

9.1 The processing of Log Files and Client Information remains subject to the applicable local law. Individuals keep any rights and remedies they may have under applicable local law.

9.2 Where these Data Processing Terms for Support Service provide more protection than applicable local law or provide additional safeguards, rights or remedies for Individuals, these Data Processing Terms for Support Service applies.

9.3 Any additional safeguards, rights or remedies granted to individuals under these Data Processing Terms for Support Service are granted by and enforceable in France against Gemalto only. Gemalto ensure that adequate steps are taken to address the implementation of these Data Processing Terms for Support Service by a Group Company.
