INTESA SANPAOLO

Prot. 2025VRSB07401

APPOINTMENT AS DATA PROCESSOR

Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council –

(hereinafter the "Regulation" or "GDPR")

Whereas:

- between the following parties

- Intesa Sanpaolo S.p.A., with registered office in Piazza San Carlo 156 - 10121 Torino, hereinafter referred to as "COMPANY" or "Controller";

  and

- Exelia S.r.l. with registered office in Str. Ionescu Crum 9 Municipio Di Brasov Regione Brasov Romania, hereinafter "Supplier" or "Processor";

  renewed the agreement for operational activities, with effect from 1st of January 2025, having as its object the provision of back office services, on behalf of the London branch of the COMPANY, in particular with regard to international branch back office (hereinafter the "Contract") which envisages, for the purposes of fulfilment of the Contract, also personal data processing (Personal data - Banking and business data), related to following data subjects: Customers, Suppliers and Employees and former employees (ISP or subsidiary banks) (hereinafter "Data"), of which the Company is the Controller.

- The Supplier, thanks to its experience, skills and reliability, is able to ensure full compliance with the provisions on the processing of personal data in terms of security and is willing to accept the appointment as personal data Processor (hereinafter the "Appointment").

Now, therefore, with this Appointment the Company, pursuant to and for the purposes of Article 28 of the GDPR,

APPOINTS

The Supplier in the person of the Legal Representative Mr. Iohn Rosanova as Data Processor for the processing activities required in fulfilment of the Contract.

In consideration of the abovementioned Appointment, the Company entrusts the Supplier with the following TASKS and provides the following INSTRUCTIONS for Data processing purposes, which the Processor shall adhere to:

1) the Data processing will be carried out by the Processor solely for the fulfilment of the Contract in a lawful and fair manner, complying with the provisions of the personal data protection legislation, the provisions of the Contract and of this Appointment, as well as any subsequent instructions provided in writing (hereinafter, collectively, the "Instructions"); it is explicitly forbidden to disseminate or disclose Data to persons who are not involved in the processing;

2) in relation to this Appointment, the Processor, in particular, shall:

   a. instruct in writing, pursuant to Article 29 GDPR, the personnel responsible to carry out operations related to the fulfilment of the Contract, providing them with detailed instructions for carrying out their duties according to the provisions of the Contract and this Appointment, thereby defining binding rules and behavior models that ensure the confidentiality and the compliance with the dissemination and disclosure

prohibition of the Data to which the employees in charge have access, and supervising their work;

b. instruct in writing, pursuant to Article 29 GDPR, those who are in possession of the characteristics of System Administrators, pursuant to the provision of the Italian Supervisory Authority (the "Supervisory Authority") of 27 November 2008 and subsequent amendments, keeping the updated list thereof available to the Company;

c. instruct in writing, in accordance with articles 37-39 of the GDPR, where the requirements are satisfied, a Data Protection Officer - "**DPO**" - providing the contact details thereof at the bottom of this Appointment;

d. should the Processor intend to entrust- after obtaining the Company's specific written authorisation - in whole or in part, the above referenced activities with any sub-contractors, whether belonging to its corporate group or not, enter into a written agreement that imposes compliance with the Instructions, thereby providing the COMPANY with a list of such sub-contractors, the methods of performance of the services rendered by them and the processing of personal data associated with such services. The Processor will limit access to the Data by the sub-contractors to the extent that this will be required for the performance of the services contractually agreed upon;

e. process the Data (directly or through sub-contractors as specified above) only within the European Union, unless the Third Country in which the Data are intended to be transferred is among those that obtained a formal adequacy decision by the European Commission (Article 45 GDPR). If, in the absence of an adequacy decision by the European Commission, the Processor intends to transfer the Data in a Third Country, according to one of the appropriate safeguards referred to in Article 46 of the GDPR or on the basis of one of the derogations provided for by Article 49 of the GDPR, the processor shall first notify the COMPANY and obtain from the latter the authorisation to transfer the Data. Even in the case of Data transfer to a Third Country, the Processor shall process the Data according to the COMPANY's Instructions. Should the transfer to a Third Country or to an international organisation be imposed by a legal obligation to which the Processor is subject, the latter shall inform the COMPANY of this obligation prior to the transfer, unless the law prohibits such information for relevant reasons of public interest.

f. adopt a **Record of Processing Activities** to track all the categories of activities and the IT applications used, in relation to the Data processing operations carried out on behalf of the Company, in full compliance with the provisions of Article 30 GDPR;

g. assist the Company in the **impact assessments** on the protection of personal data "Data Protection Impact Assessment" - "**DPIA**" - pursuant to Article 35 of GDPR and consult the Supervisory Authority in cases where the DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk pursuant to Article 36 GDPR;

h. assist the Company in ensuring Data protection through appropriate technical and organisational measures pursuant to Article 32 of the GDPR;

i. without prejudice to the contractual provisions, put in place adequate technical and organisational measures to ensure an adequate level of security to the risk of Data processing, in compliance with the provisions of Article 32 GDPR. In this regard, the Processor, also in relation to the knowledge acquired on the basis of technical and technological progress, the nature of the Data and the characteristics of the processing operations, shall take into account in particular the risks deriving from destruction, loss, modification, unauthorised disclosure of the Data or unauthorised

access, including of an accidental nature, to the Data. The technical and organisational measures include, where appropriate, pseudonymisation, obscuration and minimisation techniques, as well as protection techniques of web communication channels (e.g. https);

j. store the Data separately from those processed on behalf of other third parties, on the basis of a logical security criterion;

k. collaborate with the Company - with appropriate technical and organisational measures - so that the Company can provide the necessary feedback to the data subjects' requests concerning the exercise of the rights referred to in Articles 15-22 of the GDPR; to this end, the Processor must, within three (3) working days, inform the Company of any requests received from the data subjects, aimed at exercising the rights referred to in the above mentioned articles, and provide the Company with all the necessary elements for the related responses and the measures to be taken in this regard;

l. inform the Company of any event that may compromise the correct processing of the Data, in particular to guarantee, pursuant to Article 33 of the GDPR, in case of **Data Breach** (namely the security breach that accidentally or unlawfully leads to the destruction, loss, modification, unauthorised disclosure or access to the Data) to inform the Company without unjustified delay within 24 hours from knowledge of the breach, thereby providing every appropriate contribution and the necessary assistance for the fulfilment of the obligations required by Articles 33 and 34 of the GDPR, using, for this purpose, the attached **Information Document**;

m. immediately inform the Company, where permitted, of any request or communication from the Supervisory and/or Judicial Authority, to give adequate follow-up thereof;

n. collaborate with the Company for the implementation of the instructions that may be issued by the Supervisory Authority;

o. adopt suitable internal procedures aimed at the periodic verification of the correct application of the obligations fulfilled under the GDPR;

p. immediately inform the Company if, in its opinion, one or more of the Instructions violates the GDPR or other applicable national or European Union provisions;

q. in the event of termination of the Contract for any reason (e.g. termination, withdrawal, non-renewal at expiry), without prejudice to a different instruction provided by Company, the Processor shall return the Data and the documents processed to the Company. In the event that the Data shall be retained in order to comply with a legal obligation, the Data will be stored by the Processor solely for the purposes required by law and only for the period strictly necessary for this purpose.

3) the Data processing must be considered carried out pursuant to Article 29 GDPR, under the authority of the Company, who, at any time and with adequate notice - notice not required in the event of a Data Breach or other emergency or the need to consult with an Authority - may conduct inspections at the Supplier, and at any sub-contractors, and issue any further specific instructions for its execution; the Company may also request the provision of all the necessary information to demonstrate compliance with the Processor's obligations. The Processor, also with regard to its sub-contractors, shall provide the utmost collaboration for the Company's review activities, including inspections. The Company may also request the termination of the processing if imposed by the need to comply with legal prohibitions or obligations, or with the provisions of the Supervisory Authority and/or the Judicial Authority;

4) however, the Company reserves the right, in case of non-compliance by the Processor with the provisions referred to in Articles 1, 2 and 3 of this Appointment, the right to terminate the

Contract pursuant to Article 1456 of the Civil Code, with the consequent immediate revocation of the Appointment.

This Appointment shall be effective until the expiry date set forth in the Contract, or until the expiry date set forth in the subsequent renewals of the same Contract, or until termination of the Contract for any other reason.

It is understood that, in any case, the Appointment will continue to be effective if the parties extend the execution of the Contract, even in the absence of its formal renewal, until the end of the execution itself.

All notices provided for in this Appointment, as well as in general any communication regarding the protection of personal data, shall be sent:

- if to the Company to *Intesa Sanpaolo S.p.A. Direzione Centrale Compliance Governance, Privacy e Controlli*

  Address piazza San Carlo n°156 – 10121 Torino (Italy)

  email box dc_cgc_privacy.03263@intesasanpaolo.com

  box DPO's e-mail DPO@intesasanpaolo.com

  In the event of **Data Breach** *(Security Incidents)* also to:

- Mr. Stefano Gandolfi, e-mail: stefano.gandolfi@intesasanpaolo.com and Mr. Alberto Zoppetti, e-mail: alberto.zoppetti@intesasanpaolo.com, intern_netw_manag.03409@intesasanpaolo.com

- if to the Processor to: Exelia S.r.l.

  Registered office address: Str. Ionescu Crum 9 Municipio Di Brasov Regione Brasov Romania

  Contact:

  - name and surname: Mr. Iohn Rosanova
  - e-mail: iohn.rosanova@exeliacompany.com
  - DPO's name and surname: David Canestri
  - DPO's e-mail: dpo@intesasanpaolo.com

Yours faithfully,

Torino,

Intesa Sanpaolo S.p.A.

The Company

Exelia S.r.l.

Processor

Firmato da:
DEL VISCIO DOMENICO MICHELE
14 maggio 2026

.....

.....

Signature for acceptance

INFORMATION SET FOR EVENT NOTIFICATION

November 2021

1. INFORMATION SET

To be filled in, by the Third Party Provider with all the information available and applicable related to the specific event occurred.

GENERAL INFORMATION

General description of the event
Please, insert all the necessary information that allow to reconstruct the event occurred (in Italian or in English).

Event Timeline
1. *Date and Time of the detection[1] of the event:* _____
2. *Date and Time of the occurrence of the event, if known:* _____
3. *Date and Time of the event closure, if available:* _____

Who, inside the Company, has detected the event?			
Internal organization		***External organization***	
IT security	☐	*External auditor*	☐
IMT functions / Internal Functions (Business or Support) – Staff Member	☐	*Third party provider*	☐
		Customer/ Payment service user	☐
Internal Audit	☐	*Attacker (warning)*	☐
Other			☐

[1] *In case of data breach detected by an external provider, the Date and Time of Detection, is considered the moment when the communication from the provider arrives to the Intesa Sanpaolo Group Legal Entity competent contact point, as indicated into the agreement.*

Please specify:

1.1 EVENT TAXONOMY

Cyber Event							
Malware		***Social engineering***		***Insider/Third Party Provider event***		***Unauthorised access***	
Ransomware	☐	*Phishing / *ishing*	☐	*Accidental misuse of access rights*	☐	*Brute force attack*	☐
Trojan horse	☐	*Spear phishing*	☐	*Intentional misuse of access rights by service provider*	☐	*Malicious script injection and/or OS commanding*	☐
Virus	☐	*Pretexting*	☐	*Intentional misuse of access rights by insider*	☐	*SQL injection*	☐
Worm	☐	*Cyber squatting*	☐	*Policy violation (Insider or TPP)*	☐	*Other exploited Vulnerability*	☐
Spyware/Adware	☐	*Other social engineering*	☐	*Other Insider/TPP Threat*	☐	*Information exposure*	☐
Mobile malware	☐					*Other unauthorised access event*	☐
Other malware	☐						

Denial of Service Attack		***Other Cyber Events***		***Additional Classification**: classified as APT?*	☐
DoS	☐	*Defacement*	☐	*Please specify:*	
DDos	☐	*Brand Abuse on Mass and Social Media*	☐		
		Libel of apical persons on Mass and Social Media	☐		
		Vulnerability Scan	☐		
		Other	☐		

Operational Event							
Process failure	☐	***Accidental events*** *(e.g. human error)*	☐	***SW problem/system failure***	☐	***Sabotage (physical attack)***	☐
HW problem	☐	***Infrastructural issues*** *(Internal and external)*	☐	***Key persons / skills unavailability***	☐	***External Provider Issue***	☐
External events *(Natural, Socio political, Criminal, Transport issue, Environmental issue, Health/Sanitary, Wars/Conflict, Pandemic, Other external)*					☐	***Other operational event***	☐

Please specify:

1.2 IMPACT PERIMETER

Geographical extension			
Select the Geographical extension of the events			
International	☐	*Region*	☐
Country	☐	*City*	☐
Please specify:			

Countermeasures activated / To be activated			
Please specify if any countermeasures have been activated as a consequences of the event			
BCP activated	☐	*DRP activated*	☐
Cyber insurance	☐	*Other emergency plan activated*	☐
Other contingency measures activated	☐	*Other countermeasures activated*	☐
Other countermeasures to be activated	☐	*Please specify:*	

Overall Impact			
Which dimension have been affected by the event?			
Availability[2]	☐	*Integrity*[3]	☐
Confidentiality[4]	☐	*Authenticity*[5]	☐
Continuity[6]	☐	*Please specify*[7]*:*	

[2] *The property of process/service being accessible and usable users and customers*
[3] *The property of safeguarding the accuracy and completeness of assets (including data)*
[4] *The property that information is not made available or disclosed to unauthorised individuals, entities or processes*
[5] *The property of a source being what it claims to be*
[6] *The property of an organisation's processes, tasks and services being fully accessible and running at acceptable predefined levels*
[7] *In case of personal data, please compile the specific table for Personal Data Breach (GDPR scope).*

***Commercial Channel affected* (If Applicable)**			
Commercial channel that have been affected by the event			
Branches	☐	*Mobile Banking*	☐
E-Banking	☐	*ATMs*	☐
Telephone Banking	☐	*Point of sales*	☐
Other	☐	*If other, please specify:*	
Additional information:			

***Business Lines affected* (If Applicable)**			
Business line intended as described in 'Basel III: International regulatory framework for banks'			
Corporate Finance	☐	*Retail Brokerage*	☐
Commercial Banking	☐	*Retail Banking*	☐
Asset Management	☐	*Agency Services*	☐
Trading & Sales	☐	*Payment & Settlement*	☐
Other	☐	*Please specify:*	

***Cash Supply – Bank Account* (Applicable only to Intesa Sanpaolo S.p.A. perimeter)**			
Servizi oggetto di malfunzionamento a causa dell'evento rilevato			
Erogazione del Contante		*Servizi di base connessi alla gestione dei conti correnti*	
Gestione ATM	☐	*Saldo ed elenco movimenti*	☐
Prelievo Contanti	☐	*Operazioni di pagamento mediante carta di debito*	☐
Pagamento Pensioni	☐	*Accredito di fondi sul conto (es. deposito di contante, ricezione di bonifici)*	☐
		Addebito di fondi sul conto (es. pagamento bonifico nazionale o bonifico SEPA; addebiti diretti e addebiti ricorrenti)	☐
Informazioni addizionali:			

***Payment Service affected (PSD2 scope)* (If Applicable)**			
Payment services (as defined in annex 1 – PSD2) that are not working properly as a result of the event			
Cash placement on a payment account	☐	*Card payments*	☐
Cash withdrawal from a payment account	☐	*Issuing of payment instruments*	☐
Operations required for operating a payment account	☐	*Money remittance*	☐
Acquiring of payment instruments	☐	*Payment initiation service*	☐
Credit transfers	☐	*Account information service*	☐

Direct debits	☐	*Other*	☐
If other, please specify:			

Functional Area affected (PSD2 scope) (If Applicable)			
Steps of the payment process that have been affected by the event			
Authentication/ Authorisation	☐	*Direct settlement*	☐
Communication	☐	*Indirect settlement*	☐
Clearing	☐	*Other*	☐
If other, please specify:			

Trust Service affected (eIDAS scope) (If applicable)			
Steps of the payment process that have been affected by the event			
Electronic signature service	☐	*Electronic seal service*	☐
Electronic tile stamp service	☐	*Registered delivery service*	☐
Website authentication certificate service	☐	*Preservation service*	☐
If other, please specify:			

System & components affected			
Technological infrastructure that have been affected by the incident			
Hardware	☐	*Internet platforms*	☐
Endpoints/clients	☐	*Networking and telecommunications*	☐
Enterprise software applications	☐	*Data management and storage*	☐
Banking-related user applications/software	☐	*Other impact*	☐
If Other, please specify:			
In case of Data Breach, please provide the reference to the ISP Application Area impacted[8]:			
Additional information:			

Type of process/service disruption
Type of disruption caused by the event on service and components

[8] *To identify the application area, refer to excel file "MyAPM", column "Desc. Ambito".*

Slowdown	☐	*Malfunction (Partial Unavailability)*	☐
Total Unavailability	☐	*Other*	☐
Please specify the number of internal user that are experimenting the consequences of the event:			
Additional information:			

Type of Customers affected (If Applicable)			
The event generates any consequences on customers? If Yes, please specify the type of customer that have experimented the consequences of the event.			
Retail customers	☐	*Private customers*	☐
Corporate	☐	*Financial Institutions*	☐
Please specify:			

Personal Data Breach (GDPR scope)			
The event causes a personal data breach? If Yes, specify the Type, the Data subject and records concerned (following sections)			
Type of personal data breach			
Availability breach - accidental or unauthorized loss of access to, or destruction of, personal data.			☐
Integrity breach - unauthorized or accidental alteration of personal data.			☐
Confidentiality breach - unauthorized or accidental disclosure of, or access to, personal data.			☐
Data subject concerned			
Corporate customers	☐	*Retail/Private customers*	☐
Employees	☐	*Management*	☐
Special categories (VIP, minors, Public figures)	☐	*Other categories*[9]	☐
Please specify:			
Please specify the approximate number of data subject concerned:			
Are any third parties that process personal data involved? If yes, specify:			
Category of personal data			
Demographic personal data[10]	☐	*Banking and operational data*[11]	☐
Special categories of personal data[12]	☐	*Geolocation data*	☐

[9] E.g. Prospect customers, suppliers, promoters, employees' family, candidates, legal representatives

[10] E.g. Identification data, contact details, data related to instruction, job, personal relationship, family

[11] E.g. Data related to economical activities, commercial activities, retribution, banking, property, investment, credit card

[12] Including: sensitive data, data relating to criminal convictions and offences or related security measures, behavioural data, biometric data

Access credentials (e.g. userID, password)	☐	*Please specify:*	
Data history			
Data of the last month	☐	*Data of more than a year*	☐
Data of the last year	☐		
Personal data records concerned (Ease of identification)			
Data not identifiable	☐	*Data indirectly but uniquely identifiable*	☐
Data directly but not uniquely identifiable	☐	*Data directly and uniquely identifiable*	☐
Please specify:			
Please specify the security measures already taken to protect the data (e.g. encryption, pseudonymisation):			
Additional information:			
Kind of risk to the right and freedom for the Data Subject (potential or effective)			
Discrimination	☐	*Fraud*	☐
Damage to reputation	☐	*Limitation of rights of the data subject*	☐
Financial loss	☐	*Identity theft*	☐
Loss of confidentiality of data	☐	*Additional information:*	

Event Correlation			
Assess whether the event is connected to other events (Threat or Incident)			
Stand-alone event	☐	*Replicated occurrence of the same event*	☐
Event correlated to other event	☐	*Other*	☐
Please specify:			

General Comments on Impact Perimeter (Optional Filed)