**ANNEX: Data Processing Agreement**

**THE UNDERSIGNED:**

**The limited company NETWORK RESEARCH BELGIUM (abbreviated NRB)**, with registered office at 4040 HERSTAL, Parc industriel des Hauts-Sarts, 2e avenue, 65, with enterprise number 0430.502.430 validly represented by the undersigning person,

Hereinafter “the Processor”.

**AND:**

**The limited company/limited liability company** [Company] , with registered office at ………………………………………………………………………, with enterprise number …………………………………,

Represented by: …………………………………..,

Hereinafter “the Controller”

The Controller and Processor are hereinafter individually referred to as “Party” and together as “Parties”.

**Whereas**

1. The Processor performs information technology services for the benefit of the Controller.

Those services are framed in a contract, a set of contracts or the rules arising from the concerning public service contract(s). The reference to that/those contract(s) is named “Agreement” in this present Annex.

1. These services imply the processing of personal data for the benefit of the Controller, this within the meaning of the Belgian Privacy Act of December 8, 1992 (hereinafter: PA) and the European Regulation 2016/679 (hereinafter: GDPR”), starting May 25th, 2018.
2. The Processor only processes the personal data at the instructions of Controller, and not for his own purposes, this within the meaning of the PA and the GDPR. Within that context Processor qualifies as a data processor within the meaning of the PA and the GDPR.
3. By means of this Annex, the Parties wish to set forth their agreements regarding the processing of personal data.

**The Parties agree the following:**

1. **Definitions**

Terms such as “processing”/ "process", “personal data”, “data controller”, “data processor” and “personal data breach” shall have the meaning assigned to them in the Belgian Privacy Act (“PA”) and starting from May 25th, 2018 in the European Regulation 2016/679 (“GDPR”).

1. **Object of this Data Processing Agreement**
   1. During the performance of the Agreement, the Processor may process personal data for the benefit of the Controller in performance of the Agreement or in fulfilment of any statutory obligation. A list containing the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects is included in Appendix 1 to this Annex. The Controller is responsible for the completion of that Appendix. In case the nature of the data changes during the execution of the Agreement, the Controller will notify it to the Processor without undue delay and take charge of the costs for necessary additional security measures, this via the provided changing procedure. For every collaboration implying the processing of personal data, the Controller commits to completing a new document Appendix 1 with the envisaged processing(s). Those future processing(s) will also be governed by this Annex.
   2. The qualification of the data only lies with the Controller, who can’t hold the Processor liable in case of consequences following an error concerning the qualification of the category of processed data as indicated in the clause 2.2. The Controller commits to securing the Processor from every consequence that should follow from it.
2. **Obligations of the Processor**
   1. Processor guarantees that it, as well as any person acting under its authority, shall process personal data on documented instructions of the Controller only insofar as such shall be necessary for delivering the Performances under the Agreement (including with regard to transfers of personal data to a third country or an international organization), unless he is required to do so by Union or Member State law to which Processor is subject. In such a case, Processor will inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
   2. The Processor will not disclose personal data directly or indirectly to any person, company or governmental entity, except for what is determined under article 3.3.
   3. If such disclosure is necessary for the proper processing of personal data, this may only occur (1) after prior written permission of the Controller and then only under a full obligation of confidentiality or (2) pursuant to an order issued by a court, a governmental agency or required by the law.
   4. This Annex does not comprise consultancy services by NRB concerning data protection (like risk assessment, an evaluation of compliance with the GDPR or a classification of data), nor a posting of personnel for assistance of the Controller in his project to achieving compliance with the GDPR, particularly by taking the function of Data protection officer (DPO) or responsible for the security of information systems or the realization of awareness campaigns within the personnel of the Controller. If the Parties wish to include certain of those elements in the mission of the Processor, they will agree to that in writing and the Processor will submit a price offer in that regard.
3. **Respect of the principles applicable to the processing of personal data**
   1. Each Party conforms to all the laws and regulations applicable concerning personal data protection and particularly the PA and, after May 25th 2018, the GDPR.
   2. The Controller remains responsible of the lawfulness of the processing of the personal data, including where applicable, the obtaining of the consent of the data subjects concerned by the processing of their personal data.
   3. In case the Controller provides, manages or controls components (where applicable for example workstations linked to the services of the Processor, mechanisms to transfer data, the access and identifying information provided to his personnel), he needs to implement and maintain the technical and organizational measures required to the data protection.
4. **Security of processing**
   1. In accordance with Article 32 of the GDPR, the Processor guarantees that it will implement appropriate technical and organizational measures agreed throughout the duration of the agreement to protect against unauthorized or illegal access, loss, alteration, disclosure, processing or destruction of the Controller’s data.
   2. As part of its compliance with ISO27001 norms, the Processor is maintaining a Continuous Improvement cycle on its own organizational and technical information security measures (Information Security Management System or ‘ISMS’), of which a high level view is listed in Appendix 2 to this Annex. The ISMS ensures that any controls that would not yet be at the required maturity level are identified and that appropriate action plans are defined and implemented.

Notwithstanding the above, the level of appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the data processed is based on the information provided by the Controller in Appendix 1 of this Annex, as well as the risk assessment performed by the Controller.

Parties acknowledge also that security requirements are changing continually and that effective security requires a frequent assessment and regular improvement of outdated security measures. The Processor will estimate the cost of additional and conceivable measures for improvement spontaneously or at the suggestion of the Controller, the decision to implement them or not remaining with the Controller who will cover the cost of those measures via the changing procedure.

* 1. The Processor informs its employees and agents of the obligations resting on the Processor with regards to Controller Personal Data. The Processor makes all employees and agents involved in the processing of Controller Personal Data, enter into obligations of confidentiality with the purpose of safeguarding the confidentiality and integrity of Controller Personal Data.

1. **Compliance** 
   1. DPO

Processor has designated a data protection officer of whom the coordinates are included in Appendix 3, which doesn’t mean that the Processor considers himself obligated to do so in accordance with article 37 of GDPR.

* 1. Impact assessment

The impact assessment is carried out by the Controller. On request of the Controller, in accordance with the articles 28 and 35 of the GDPR, the Processor shall cooperate in preparing a data protection impact assessment as well as in regular updating that assessment. The Parties will agree to the costs of that assistance.

If necessary, the Processor will adapt its technical and organizational measures, at the costs of the Controller, in accordance to the results of the assessment and after decision in that sense of the Controller, this via the changing procedure. If no agreement is reached, the services cannot be performed.

* 1. Rights of data subjects

On the basis of article 28 of the GDPR, the Processor, taking into account the type of processing, assists the Controller by way of appropriate technical and organizational measures in every possible way, in carrying out his obligation of responding to the requests addressed to him by data subjects in order to exercise their rights provided in chapter III of the GDPR.

The Processor will notify without undue delay to the Controller any complaint, request or notice from a data subject exercising his rights under data protection legislation.

The Controller will take care of all relations with the data subject.

The Controller will have to specify to the Processor if a time limit is allotted to the Controller in order to respond to the data subject. In any event, the Controller will formulate his request for assistance to the Processor as soon as he receives the request of the data subject and will make sure that the Processor disposes of a time limit of at least 25 days to answer his request.

Every assistance provided by the Processor to the Controller in that context will be invoiced in accordance with the terms of article 6.6.

* 1. The development of additional measures for implementation to existing measures, will be carried out at costs of the Controller, via the changing procedure.
  2. Demonstration of respect of the obligations and audit

Starting May 25th 2018, the Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down by Belgian law and GDPR, including in what concerns all necessary information to enable the carrying out of audits, or inspections, by the Controller or another auditor, appointed by him, and contribute to those audits. Every audit will be carried out in accordance with the audit clause of the agreement and at all times with a prior notice of 2 weeks at least.

* 1. Terms of assistance

Any assistance from the Processor under Articles 6.3 and 6.5, without prejudice to what is provided for by the Parties regarding the invoicing of audits, shall be invoiced to the controller based on an hourly rate of 116,30 €/hour (for any profile), annually reviewed in January on the basis of the formula *Reviewed rate* = *116,30€ \*(0,2+0,8\*S1/S0)* with the last index of the month of September « Agoria- Salary cost (+10 workers)- national average » in force at the date of signature of the present Annex, as reference value (S0).

1. **Location of processing**

7.1 The Processor shall only process the Controller’s Personal Data, whether this is done by himself or via a third party, at a location in the EU.

Nevertheless, in exceptional situations, such as level 3 or 4 support interventions and to ensure the continuity of services, the Controller accepts and agrees that a transfer to a third country can take place, given the taking of appropriate safeguards by the Processor in compliance with the obligations of the GDPR.

1. **Personal data breach management**
   1. In case of a personal data breach in the context of their processing, the Processor will assist the Controller in ensuring compliance with the obligations pursuant to Belgian law and to GDPR Article 32 to 36, taking into account the nature of processing and the information available to the Processor. If the Controller judges it necessary, he will inform the data subjects and third parties, including the Data protection Authority, of the data breach.
   2. The Processor notifies each personal data breach to the Controller as soon as possible after having knowledge of them.
   3. Processor will document personal data breaches, comprising the facts relating to the personal data breach, any useful information on the origin, nature, scope and consequences of the Incident, the remedial actions that have been or shall be taken and all relevant information. Processor shall share this information with the Controller so that the Controller is in a position to comply with the requirements of the data protection legislation regarding (1) information of the competent authorities and of the data subjects, and (2) the implementation of all necessary remedies.
   4. Processor will make its best efforts to reduce or remedy as soon as possible any negative consequences arising from a personal data breach.
   5. The obligation for one Party to make a report or respond to a personal data breach is not and will not be interpreted as a recognition for that Party of any fault or responsibility regarding that breach.
2. **Use of subProcessors**
   1. In accordance with article 28.2 of the GDPR, the Processor will not engage another processor without prior written authorization of the Controller. The Controller hereby grants a general authorization to the Processor to use subProcessors in the provision of services to the Controller.
   2. The Controller has knowledge of subProcessors existing or active before the signature of the present Annex (such as IBM, Microsoft, Oracle, SAP, Dell, Cisco, VMware, Compuware, etc.), and on which he agrees. At the request of the Controller, the Processor will provide the list of subProcessors. The Processor will inform the Controller in case of recourse to a future subProcessor. The Controller will, if necessary, issue reasonable and justified objections within 15 days after this information.
   3. In accordance with article 28.4 of the GDPR, the Processor shall use only SubProcessors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing shall meet the requirements of this Annex and of Belgian law and GDPR and ensure the protection of the rights of the data subject.
   4. Processor will impose upon its subProcessor(s) the same binding or even more binding commitments as those arising from this Annex.
3. **Liability**
   1. The Parties comply with article 82 of the GDPR concerning the right to compensation and liability. However, it is explicitly agreed to that the liability of the Processor is limited in accordance with that specified in the Agreement.
   2. The Controller secures the Processor from any consequence (in particular the costs of additional performances of the Processor, the suffered damage, administrative fines, every sum due to a data subject or to a subProcessor) resulting from:

* an erroneous qualification of the data and details of the processing, as foreseen in article 2
* in case of absence of complete information of the Processor by the Controller, particularly concerning a personal data breach, a request from a supervisory authority or a data subject
* a decision being the responsibility of the Controller or every breach committed by the personnel of the Controller.
* and more generally a breach of obligations put under the responsibility of the Controller by the applicable legislation or the Agreement.
  1. When the Controller or Processor has completely repaired the damage suffered by the data subject, he has the right to claim from the other party, that part of the reparation corresponding to his part of responsibility for the damage, provided that the other party has agreed to the adequate nature of the indemnification of the data subject or provided that the indemnity has been fixed by a judgment and the other party has been implicated in the legal proceeding.

1. **Return and deletion of Personal Data**

Within 3 months after the end of the Agreement or at first request from the Controller, the Processor shall at Controller’s discretion:

* + 1. delete all copies of Controller Personal Data stored or processed by The Processor,
    2. or return all the personal data to the controller and deletes existing copies, in which case he will have to defray the Processor,

unless Union or Member State law requires storage of the personal data.

1. **Processing of the co-contracting party’s Personal Data**
   1. Personal data of the contact persons of a Party (surname, first name, function, telephone and fax number, e-mail, languages ) are processed by the other Party in accordance with the applicable legislation regarding the processing of personal data, to enable the entering into and good performance of the Agreement (comprising the order, the performance, the invoicing, reporting, security) as well as for purposes of direct marketing Furthermore, by supplying its personal data, every Party gives the other Party express permission to process this information for and to the extent necessary for the purposes indicated above.

If one Party communicates the personal data of his employees to the other Party, he shall ensure that he obtains and communicates proof of the consent of his employees to the Party. These data shall be used exclusively for the purposes listed above, unless opposition later on, on behalf of the other Party on the purpose of direct marketing.

* 1. The personal data that the Parties communicate are stored in a file of which the other party is the master and responsible for the processing.
  2. The personal data, as referred to in this article, shall be stored for 10 years after the end of the concerned contract.
  3. The Parties or their contact persons may obtain, free of charge if it is a reasonable volume, from the Controller the written communication of the data and the portability of the data, as well as, where appropriate, rectification, restriction of processing, deletion of those which are inaccurate, incomplete or irrelevant. The application is considered as dismisses where no action has been taken on the application within 30 days of the request. They may also apply to or lodge a complaint with the Data protection Authority for the exercise of these rights.

Location: ……………………………..

Date: ……………………………..

In two originals, of which every party receives one.

[Company] NRB

The Controller The Processor

Name and title Name and title

**APPENDIX 1: Personal data to be processed and purposes**

<The charts are to be completed as many times as there are processing(s)>

This appendix is an integral part of the Agreement concluded between:

The « Controller »: [Company]

And the « Processor »: Network Research Belgium (abbreviated N.R.B.)

Reference service contract/project: ………………….

Subject-matter of the processing:

Duration of the processing:

Nature of the processing:

Purpose of the processing:

Type of personal data:

………

Of which (tick the appropriate mentions):

🞎 A: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of data concerning a natural person's sex life or sexual orientation

🞎 B: data concerning health or genetic data, biometric data for the purpose of uniquely identifying a natural person

🞎 C: personal data relating to criminal convictions and offences or related security measures

🞎 D: personal data relating to disputes submitted to the courts and tribunals as well as administrative jurisdictions, relating to suspicions, legal proceedings or convictions relating to infringements or relating to administrative sanctions or security measures

🞎 E: national registry number, protected under the Belgian law of August 8, 1983

🞎 F: others to specify…

Categories of data subjects:

Subject-matter of the processing:

Duration of the processing:

Nature of the processing:

Purpose of the processing:

Type of personal data:

Of which (tick the appropriate mentions):

🞎 A 🞎 B 🞎 C 🞎 D 🞎 E 🞎 F: others to specify…

Categories of data subjects:

Subject-matter of the processing:

Duration of the processing:

Nature of the processing:

Purpose of the processing:

Type of personal data:

Of which (tick the appropriate mentions):

🞎 A 🞎 B 🞎 C 🞎 D 🞎 E 🞎 F: others to specify…

Categories of data subjects:

Since only the Controller disposes of all necessary information in order to complete this annex, it is his responsibility to do so.

His attention is drawn to the fact that he cannot hold the Processor liable in case of consequences following any error in the information contained in this Appendix, and especially relating to the type of processed data.

……………………………..

Date and signature

For the Controller

**APPENDIX 2: Standard technical and organizational security measures applicable to the ISMS of the Processor**

# Overall security and access control organization

| Key Control | Overview of technical and organizational measures |
| --- | --- |
| (general reference to ISO27K controls domain 5.1.x Information Security Policies) : maturity & ongoing maintenance thereof through ISMS | * Information Security policy is in place and monitored, security objectives are defined in view of the business strategy and information security risk assessment * Privacy and Data Protection policy is in place and monitored |
| (general reference to ISO27K controls domain 6.1.x Organization of Information Security) : organization and roles & responsibilities | * Security Officer is in place * A network of Information Security Coordinators and ‘Relais’ is in place, responsibilities are defined * Data Protection Officer is in place * (for project management) Information security objectives are included in project objectives |
| (general reference to ISO27K controls domain 8.x) Asset Management / Inventory | * Data Classification policy is in place and monitored * An inventory of IT/information assets is in place, asset ownership is defined * IT/information assets are classified in view of their criticality (criteria in Data Classification policy) |
| (general reference to ISO27K controls domain 18.1.x) Compliance / Compliance monitoring) | * Compliance policy is in place and monitored * (+ implied in continuous improvement ISMS, monitoring of other Information Security policies) |
| (ISO27K 9.1.x) Access control policy, Access to networks and network services | * Access control policy is in place and monitored, and covers both logical and physical access to information assets * Access to information assets is based on need-to-know / need-to-use principles * Access to NRB network / network services is subject to technical and management controls, to ensure only authorized users can gain access (cf. also further : user management, authentication mechanisms, …) * Use of network services is monitored. |
| (ISO27K 9.2.x, 9.3.x) User Access Management, Use of secret authentication information | * User registration and de-registration: process to assign, enable and revoke user IDs is defined. The use of shared user IDs is only permitted in exceptional circumstances, when necessary for business or operational reasons * User Access provisioning: access rights are formally assigned to defined users on a need-to-know / need-to-use basis. Access is changed / revoked if users change functions or leave the company. * Privileged access rights are restricted to appropriate personnel (e.g. administrators). Use of privileged access is subject to specific procedures, and activity is logged and monitored * A formal process is in place to allocate secret authentication information to users (mandatory change upon first use, minimum password requirements …). Identity verification is in place in case a user’s authentication information needs to be renewed / replaced * Users receive instructions on the use of their authentication information (obligation to maintain secrecy/confidentiality thereof, avoiding records, prohibition to share, …) * User access rights are reviewed at regular intervals, and also upon role changes. Access rights are removed or adjusted as required |
| (ISO27K 9.4.x) System and Application access control | * Access to systems and applications is restricted, in line with the principles defined in the access control policy * Where required, access to systems and applications is subject to secure log-on procedures (authentication process, protection of passwords during log-on procedure, logging & monitoring of failed attempts, termination of idle sessions) * The password management system enforces high-quality passwords (minimum length, type of characters, change of password upon first logon, change of password at regular intervals, restrict re-use of old passwords …). * For privileged users and utility programs, additional security requirements are established, and all activity is logged and monitored (i.e., not only logon process activity). * Application source code and related assets is tightly restricted, and any access to source code libraries is logged and monitored |

# Secure Operations

| Key Control | Overview of technical and organizational measures |
| --- | --- |
| (general reference to ISO27K controls domain 11.1.x Secure Areas) : physical security perimeter, access controls, ... | * Overall building security includes physical barriers, a badge-based access control, video surveillance, … * Access to identified ‘secure areas’ (e.g. data centre) is further restricted to authorized personnel only. Any visitors (e.g. technical staff from suppliers) are identified up-front (white list principle), and receive temporary access only |
| (general reference to ISO27K controls domain 11.2.x Equipment handling) : equipment protection, maintenance, removal/disposal practices, ... | * Equipment is held in areas that are protected against environmental threats (fire, water, theft, …) * Procedures for the secure removal and disposal of information assets are established and monitored |
| (ISO27K 12.1.x) Operational procedures and responsibilities | * Operating procedures are documented and available to all users who need them. The procedures cover system installation / configurations, backup and recovery management, scheduling (if applicable), error handling, overall monitoring * Formal change management is set up to handle changes to infrastructure / procedures / organization in a standardized manner (documentation, authorization, testing & final approval, implementation) * Emergency changes are subject to explicit review and approval * Capacity management/Performance monitoring is defined and operational (projections for future capacity requirements, deletion of obsolete data, multiple performance optimization measures) * Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. * Preventive and detective measures against malware are operational. |
| (ISO27K 12.3.x) Backup, archiving and destruction principles are defined and implemented, and tested on a regular basis | * Physical backup procedures are defined, monitored and tested regularly * Logical backup and restore procedures are defined, monitored and tested regularly * Archiving procedures are defined and monitored * Backup information is subject to physical and environmental protection * Destruction of backups and archives is conducted as per defined procedures |
| (ISO27K 12.4.x) Event logging | * Event logging is established - both overall & specifically for administrator activity (overall logs capture events, administrator logs full detail of activity) |
| (ISO27K 12.5.1) (System) Software installation is subject to standardized and secure practices | * Only administrators have the authorization and access profiles to conduct system software installation or upgrades * Installations are subject to formal procedures, that enforce adequate testing prior to actual installation * A rollback strategy is defined for any system software upgrade |
| (ISO27K 12.6.1) Technical vulnerability management | * Preventive and detective measures against technical vulnerabilities are operational (starting from an inventory of IT assets and risk-based classification thereof) * A patching schedule is defined and adhered to * If new vulnerabilities are identified, a risk assessment takes place and actions defined * Restrictions on software installation by users are in place |
| (ISO27K 16.1.x) Incident Management | * Incident Management policy and procedures are established and monitored, roles & responsibilities are defined * The incident handling process includes principles and guidance on escalation and reporting, the assessment & response mechanism, lessons-learned practices, documentation requirements * Specifically for (potential) security and privacy-related incidents, additional escalation and analysis requirements are established |

# Secure Development

| Key Control | Overview of technical and organizational measures |
| --- | --- |
| (ISO27K 14.1.1) Security requirements analysis and specifications | * Information security requirements are defined for any new information system / application being considered for implementation / development (including e.g. authentication and access principles depending on the criticality of the information, logging requirements, training of to-be users, …) * Additional security requirements are defined and implemented for any new system / application that makes use of public infrastructure / networks (including e.g. extra authentication steps, encryption, confirmation processes for data integrity, …) * Additional security requirements are defined and implemented for any new system / application that involves operational transactions (including e.g. electronic signatures, authentication, privacy considerations, encryption of communication, …) |
| (ISO27K 14.2.x) Secure development | * A secure development policy is established and monitored * Secure Development training is provided to all developers, covering secure design, coding and testing principles and practices. * Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. * Formal change control procedures are applied for any changes to systems / applications : authority levels are defined & adhered to, version control is applied * Testing and test acceptance procedures are defined and adhered to – at different stages of development, and ultimately in formal user acceptance testing (including explicit testing of security and other ‘non-functional’ requirements), * Specifically when underlying operating platforms are changed, also all critical applications using these platforms are reviewed and tested * Specifically when NRB uses other suppliers to assist in development activities (partial or full outsourcing), secure development practices (design, coding, testing) are enforced contractually. |
| (ISO27K 14.3.1) Protection of test data | * Development, Test and Operational environments are separated. Procedures for transferring software between these environments are established and monitored. * Test data is selected based on testing needs – only under exceptional circumstances will operational data be used in test (or development) environments (such operational data is deleted once testing is completed) * Test environments are subject to standard access control procedures |

**APPENDIX 3: DPO and contact details**

Data Protection Officer of the Processor:

Name + Surname: Claudia Grosu

Address: Parc Industriel des Hauts Sarts - 2e avenue 65 | 4040 Herstal

Mail: dpo@nrb.be

Tel: +32 (0)4 249 70 26

Data Protection Officer of the Controller:

Name + Surname: …………………………..

Address: ………………………………………………………………………….

Mail: ……………………………………………

Tel: ……………………………………………..

Below are the contact details of Controller’s staff member who must be contacted in the event of “incidents”/personal data breaches.

|  |  |
| --- | --- |
| Name: |  |
| Title: | Data Protection Officer |
| Telephone number: |  |
| e-mail: |  |

|  |  |
| --- | --- |
| Name: |  |
| Title: | Security Counsellor for the Information System |
| Telephone number: |  |
| e-mail: |  |