



THE SAMRES GROUP

BINDING CORPORATE RULES FOR PROCESSORS

Table of Contents

1	Introduction	3
2	Definitions	4
3	Documents	6
4	Material Scope	6
5	Data Processing Agreement	6
6	Sub-processing	6
7	Cooperation.....	7
8	Compliance.....	8
9	Transparency.....	10
10	Security.....	12
11	Liability	12
12	Training Program.....	13
13	Data Protection Officer	13
14	Audit Program	14
15	Third Party Beneficiary Rights	15
16	Complaint Handling Procedure	17
17	Updates	18
18	Governing Law.....	19
19	Invalidity	19

BINDING CORPORATE RULES FOR PROCESSORS

The Binding Corporate Rules for Processors ("BCR-P") are entered into between the following members of the Samres Group:

- 1) Samres AB, reg. no. 556433-7417, Västra Stationstorget 10, 222 37 Lund, Sweden ("Samres");
- 2) Samreis Eesti AS, reg. no. 11055561, Kõüni 5B, Tartu, EE-51003, Estonia ("Samreis Eesti");
- 3) Samres South East SRL, reg. no. 1007600039103, Str. Banulescu-Bodoni 27/1, MD-2005, Chisinau, Moldova ("Samres South East"); and
- 4) Samres Senegal SUARL, reg. no. 004337178, Boulevard de l'Est X 2, bis Point E Immeube Adjia Koone, BP 10700 Dakar, Senegal ("Samres Senegal").

1 INTRODUCTION

- 1.1 The company structure of the Samres Group and the contact details of the members of the Samres Group are specified in Appendix 1.
- 1.2 The members of the Samres Group regularly enter into Data Processing Agreements regarding Processing of Personal Data on behalf of government bodies and external companies acting as Controllers. Personal Data received from government bodies and external companies are Processed by members of the Samres Group acting as Processors or Sub-processors. Members of the Samres Group established within the EEA regularly transfer Personal Data for Processing to members of the Samres Group established outside the EEA. The purpose of the BCR-P is to ensure that there is an adequate level of protection for the transferring and Processing of Personal Data by members of the Samres Group established outside the EEA.
- 1.3 Each member of the Samres Group and their employees have a duty to respect the BCR-P when Processing Personal Data on behalf of the Controller. Each member and their employees must also respect the Instructions from the Controller with regard to the Processing of Personal Data and the security and confidentiality measures as provided in the Data Processing Agreement (see Articles 28, 29 and 32 of the GDPR in Appendix 4).

A group member acting as importer that ceases to be bound by the BCR-P may keep, return, or delete the data. If the exporter and importer agree that the data may be kept by the importer, protection must be maintained in accordance with GDPR

regarding *Transfers on the basis of an adequacy decision* (Article 45) or *Transfers subject to appropriate safeguards* (Article 46) unless one of the derogations for specific situations pursuant to Article 49 in the GDPR applies (see Articles 45, 46 and 49 of the GDPR in Appendix 4).

- 1.4 The BCR-P applies to all Processing of Personal Data Processed for Processor activities within the Samres Group for when members of the Samres Group act as Processors for the Controller, whatever the origin of the Personal Data from the Controller.

2 DEFINITIONS

- 2.1 Definitions and terms used in this document are defined as set forth below, unless circumstances indicate otherwise. Any term that is used in the GDPR and that is not stated below is defined in accordance with Article 4 in the GDPR.

"Binding Corporate Rules for Processors"	Personal Data protection policies which are adhered to by a Processor established on the territory of a Member State for transfers or a set of transfers of Personal Data to a Processor in one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
"Controller"	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by European Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by European Union or Member State law.
"Data Processing Agreement"	A contract between the Controller and the Processor as well as between the Processor and the Sub-processor that adheres to the provisions set up in Article 28 in the GDPR.
"Data Subject"	The living identifiable natural person, whose Personal Data is Processed.
"EEA"	The European Economic Area, including the European Union, Norway, Iceland and Lichtenstein.
"GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

	regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation").
"Instruction"	The documented instructions, which the Controller gives within the scope of a Data Processing Agreement.
"Member State"	A country that is member of the European Union.
"Personal Data"	Any information relating to an identified or identifiable natural person ("Data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
"Personal Data Breach"	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.
"Processing"	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"Processor"	A natural or legal person, public authority, agency, or other body, which Processes Personal Data on behalf of the Controller.
"Samres Group"	The members of the Samres Group that are bound by the Binding Corporate Rules for Processors.
"Sub-processor"	A natural or legal person, public authority, agency, or other body, hired by the Processor which Processes Personal Data on behalf of the Controller.

“Supervisory Authority”	An independent public authority, which is established by a Member State pursuant to Article 51 in the GDPR.
“Third Country”	A country outside the EEA.
“Third Party”	A natural or legal person, public authority, agency, or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to Process Personal Data.

3 DOCUMENTS

- 3.1 The BCR-P comprises this document as well as Appendix 1 (Company Structure and Contact Information), Appendix 2 (Material Scope and Transfers) Appendix 3 (Training Program) and Appendix 4 (Excerpts from the GDPR).
- 3.2 In the event of any contradiction between this document and the appendices, this document takes precedence, unless circumstances clearly stipulate or indicate otherwise.

4 MATERIAL SCOPE

- 4.1 The expected nature of data transferred including the categories of Personal Data, anticipated types of Processing and its purposes, types of Data Subjects concerned by the transfers, and the identification of the relevant Third Countries is specified in Appendix 2.

5 DATA PROCESSING AGREEMENT

- 5.1 The BCR-P is made binding towards the Controller and the Processor as well as between the Processor and the Sub-processor through a special attachment of the BCR-P or a specific reference with the possibility of electronic access to the BCR-P in the Data Processing Agreements, which complies with Article 28 in the GDPR.

6 SUB-PROCESSING

- 6.1 The members of the Samres Group cannot Process Personal Data as Sub-processors without the prior informed specific or general written consent from the Controller. The Instruction from the Controller must specify if a general authorization is given for all new internal Sub-processors or if a specific authorization is required for each new internal Sub-processor. If a general authorization is given, the Controller must be

informed by the Processor of any intended changes concerning the addition or replacement of internal Sub-processors in such a timely fashion that the Controller can object to such changes or to terminate the agreement before Personal Data is transferred to the new internal Sub-processors.

6.2 The external Sub-processors can only Process Personal Data with the prior informed specific or general written authorization of the Controller. The Instruction from the Controller must specify if a general authorization is given for all new external Sub-processors or if a specific authorization is required for each new external Sub-processor. If a general authorization is given, the Controller must be informed by the Processor of any intended changes concerning the addition or replacement of external Sub-processors in such a timely fashion that the Controller can object to such changes or to terminate the agreement before Personal Data is transferred to the new external Sub-processor.

6.3 If a member of the Samres Group engages a Sub-processor for carrying out specific processing activities on behalf of the Controller, it shall do so only by way of a contract or other legal act under European Union or Member State law with the sub-processor. That member of the Samres Group must make sure that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46 and 47 in the GDPR as well as ensure that the same data protection obligations as set out in the Data Processing Agreement with the Controller and Sections 15.1, 15.2, 15.3, 15.4, 5, 7.1, 7.5, 8.1, 8.2, 7.2, 7.3, 10, 18.1, 7.4, 6, 8.3, 8.4, 8.5, 1.1 and 9 in the BCR-P are imposed on the Sub-processor by way of a Data Processing Agreement with that Sub-processor (see Articles 28, 29, 32, 45, 46 and 47 in Appendix 4). The member of the Samres Group must also attest that sufficient guarantees to implement appropriate technical and organizational measures are provided in such a manner that the Processing meets the requirements in Article 28.4 in the GDPR.

7 COOPERATION

7.1 The Processors and Sub-processors have a duty to cooperate, help and assist the Controller to comply with European Union and Member State data protection law. Any cooperation with and assistance to the Controller must be done within a reasonable time and to the extent reasonably possible.

7.2 The Processors and Sub-processors must, in particular, execute the necessary measures, when asked by the Controller, in order to have Personal Data updated, corrected or deleted. The Processors and Sub-processors must also inform each

member of the Samres Group to whom the Personal Data has been disclosed about any rectification or deletion of Personal Data.

- 7.3 The Processors and Sub-processors must, in particular, execute the necessary measures, when asked by the Controller, in order to have Personal Data deleted or anonymised from the moment the identification form is not necessary anymore. The Processors and Sub-processors must also inform each member of the Samres Group to whom the Personal Data has been disclosed about any deletion or anonymisation of Personal Data.
- 7.4 The Processors and Sub-processors must, in particular, execute the appropriate technical and organizational measures, when asked by the Controller, in order to help fulfill the obligation of the Controller to respond to requests from Data Subjects who wish to exercise their rights as set out in Articles 12 to 23 in the GDPR (see Articles 12 to 23 in Appendix 4), including communicating any useful information in order to help the Controller comply with its duty to respect the rights of the Data Subjects (in accordance with Article 28.3.e in the GDPR, article can be found in Appendix 4). The Processors and Sub-processors must transmit to the Controller any request from the Data Subjects without answering that request, unless they are authorized to do so by the Controller.
- 7.5 The members of the Samres Group have a duty to cooperate with and accept to be audited by the Supervisory Authorities competent for the relevant Controller, and to taking into account the advice and to abide by decision of these Supervisory Authorities on any issue related to the BCR-P.

8 COMPLIANCE

- 8.1 The Processors can only Process Personal Data on behalf of the Controller and in compliance with the documented instructions from the Controller, including with regard to transfers of Personal Data to Third Countries. The Processors can Process Personal Data beyond the Instructions from the Controller if they are required to do so by European Union and Member State law, in which case they must inform the Controller about the legal requirement before the Processing takes place. The Processors cannot inform the Controller about the legal requirement if they are prohibited from doing so on important grounds of public interest (in accordance with Article 28.3.a in the GDPR, article can be found in Appendix 4). The Controller that has been informed about the legal requirement is then entitled to suspend the transfer of Personal Data and terminate the agreement.
- 8.2 If the Processors or Sub-processors cease to Process Personal Data on behalf of the Controller, they must, at the choice of the Controller, delete or return all Personal Data transferred to the Controller as well as delete the copies thereof, certifying to the

Controller that they have done so. Members of the Samres Group are not required to delete or return all Personal Data as well as the copies thereof if legislation imposed upon them requires storage of the Personal Data transferred, in which case the Processors and Sub-processors must inform the Controller and certify that they will keep the confidentiality of the Personal Data transferred and not actively Process the Personal Data anymore.

8.3 The Processors must make available to the Controller all information necessary to demonstrate compliance with their obligations as provided by Article 28.3.h in the GDPR and allow for and contribute to external data protection audits, including inspections conducted by the Controller or another auditor mandated by the Controller (Article 28.3.h can be found in Appendix 4). The Processors must also immediately inform the Controller if in their opinion an Instruction from the Controller infringes on GDPR or other European Union or State Member data protection provisions.

8.4 The members of the Samres Group must, in order to demonstrate compliance, maintain a record of all categories of Processing activities carried out on behalf of each Controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards (see Article 49(1) in Appendix 4);
- where possible, a general description of the technical and organisational security measures referred to in Article 32.1 in the GDPR (see Article 32.1 in Appendix 4).

The record must be maintained in writing and in electronic form as well as be made available to the Supervisory Authorities upon request.

8.5 The members of the Samres Group must assist the Controller in implementing appropriate technical and organizational measures to comply with data protection principles as well as facilitate compliance with the requirements set up by the BCR-P in practice. In particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default (Article 25 in the GDPR, see

Appendix 4), legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules (Article 47.2.d in the GDPR, see Appendix 4).

9 TRANSPARENCY

9.1 The Samres Group will use the BCR-P as a tool for transfers only where they have assessed that the law and practices in the third country of destination applicable to the processing of the personal data by the member of the group acting as importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under the BCR-P.

The members of the Samres Group shall make an analysis of the legislation taking into account elements such as:

- the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
- the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
- any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the BCR-P, including measures applied during transmission and to the processing of the personal data in the country of destination.

If a member of the Samres Group finds that any safeguards in addition to those envisaged under the BCR-P should be put in place, they must without undue delay inform and involve the Controller, the members of the group in the EEA and the data protection officer in the assessment. The assessments and any eventual supplementary measures selected and implemented shall be documented and available to the competent supervisory authority upon request.

If a member of the Samres Group has reasons to believe that existing or future legislation applicable to it prevents it from fulfilling the instructions received from the Controller or its obligations under the BCR-P or the Data Processing Agreement, it must inform Samres AB and the data protection officer. Samres AB, with the help of the data protection officer, shall promptly identify appropriate measures to be adopted by the members of the Samres Group in order to enable them to fulfil the BCR-P, and to inform the members of the Samres Group and the Controller about the analysis. If effective supplementary measures cannot be put in place or if instructed by the competent supervisory authority, the Controller is then entitled to suspend the transfer of data and terminate the agreement. Personal data that has been transferred prior to the suspension, and any copies thereof, should at the choice of the Controller be returned to it or destroyed in their entirety.

A member of the Samres Group acting as an exporter must on an ongoing basis, and where appropriate in collaboration with Controllers and data importers, monitor the development in the third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

- 9.2 The members of the Samres Group must immediately inform the Controller about any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body. The members of the Samres Group do not have to inform the Controller about the request if they are prohibited to do so by the enforcement authority or state security body. In any case, the members of the Samres Group must put the request for disclosure on hold and inform the Supervisory Authority competent for the Controller and the Supervisory Authority competent for the Processor about the request. The information that is provided to the Supervisory Authorities must include details about the data requested, the requesting body and the legal basis for the disclosure. If the members of the Samres Group are prohibited from informing the Controller or the Supervisory Authorities, they must use their best efforts to obtain the right to waive the prohibition in order to communicate as much information as they can and as soon as possible to the Controller and the Supervisory Authorities. The members of the Samres Group must be able to demonstrate that they tried to obtain such a waiver. If the members of the Samres Group, despite having used their best efforts, are not able to inform the Controller and the Supervisory Authorities, they must annually provide the Controller and the Supervisory Authorities with general information about the requests they receive from the enforcement authority or state security body (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the

outcome of such challenges, etc.). No personal data is stored locally in a third country, see Appendix 2.

- 9.3 In any case, transfers of Personal Data from a member of the Samres Group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that goes beyond what is necessary in a democratic society.

10 SECURITY

- 10.1 The Processors and Sub-processors have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing. These security measures must at least meet the requirements of the member state data protection law applicable to the Controller as well as any existing particular measures specified in the Data Processing Agreement.
- 10.2 The Processors and Sub-processors have a duty to assist the Controller in ensuring compliance with the security obligations set out in Articles 32 to 36 in the GDPR (see Articles in Appendix 4) taking into account the nature of Processing and the information available to the Processors (in accordance with Article 28.3.f in the GDPR, Article can be found in Appendix 4).
- 10.3 The Processors have a duty, insofar as possible, to immediately inform the Controller after becoming aware of any Personal Data Breach. The Sub-processors must also without undue delay inform the Processor and the Controller after becoming aware of any Personal Data Breach.
- 10.4 The Controller has the right to enforce the BCR-P against any members of the Samres Group that cause a violation of the BCR-P, and, moreover, against Samres AB in case any member of the Samres Group or external Sub-processor established outside the EEA violates the BCR-P or the Data Processing Agreement.

11 LIABILITY

- 11.1 Samres AB accepts responsibility for and agree to take the necessary action to remedy any violation of the BCR-P caused by members of the Samres Group or external Sub-processors established outside the EEA as well as pay compensation for any damage resulting from such violations. Samres AB accepts this responsibility as if it itself had committed the violation in Sweden. Samres AB cannot rely on a violation of the BCR-P by a Sub-processor of its obligations in order to avoid its own responsibilities.
- 11.2 Samres AB has the liability to prove that the member of the Samres Group or external Sub-processors established outside the EEA is not responsible for any violation of the BCR-P, which has resulted in the Data Subject claiming damages. If the Controller can

demonstrate that it has suffered damage and establish facts which show it is likely that the damage has occurred because of a violation of the BCR-P, Samres AB has the liability to prove that the member of the Samres Group or external Sub-processors established outside the EEA is not responsible for the violation of the BCR-P giving rise to those damages and that no such violation took place. If Samres AB can demonstrate that the member of the Samres Group established outside the EEA is not responsible for the violation of the BCR-P, Samres AB can discharge itself from any responsibility/liability.

12 TRAINING PROGRAM

- 12.1 The members of the Samres Group ensures that appropriate training on the GDPR and the BCR-P is provided to personnel who have permanent or regular access to Personal Data, who are involved in the collection of Personal Data or who are engaged in the development of tools used to Process Personal Data. The training program is specified in Appendix 3.

13 DATA PROTECTION OFFICER

- 13.1 A data protection officer is appointed with the responsibility to monitor the compliance of the Samres Group with the BCR-P (in accordance with Article 37 in the GDPR, see Article in Appendix 4).
- 13.2 The data protection officer enjoys the highest management support and reports directly to the board of management of the Samres Group (in accordance with Article 38.3 in the GDPR, see Article in Appendix 4).
- 13.3 The data protection officer has, at least, the following duties:
- Monitor the proper implementation of and compliance to the BCR-P;
 - Inform and advise the board of management of the Samres Group on the implementation of and compliance to the BCR-P;
 - Develop a data protection training program as well as ensure and monitor that the personnel are appropriately educated about data protection in accordance to that training program;
 - Decide on an internal data protection audit program, ensure that internal data protection audits are regularly carried out, address internal data protection audit findings and communicate them to the board of management of the Samres Group;

- Monitor requests from Data Subjects and ensuring that they are referred to the relevant Controller;
- Deal with external data protection audits and investigations from Supervisory Authorities and Controllers;
- Communicate with Supervisory Authorities and Controllers about data privacy issues;
- Monitor that Personal Data Breaches are reported to the Controller and that appropriate measures are taken to alleviate and prevent future Personal Data Breaches; and
- To keep a fully updated list of the BCR-P members and to track and record any update of the BCR-P.

13.4 The data protection officer is assisted by an internal team called “Samres Data Protection Committee”. The Samres Data Protection Committee consist of Samres data protection officer, CEO, and CTO. The Samres Group employs a legal assistant in periods depending on the workload, this resource also joins the team when working.

The Samres Data Protection Committee has regular meetings discussing the Samres Group’s data protection work and what recourses/assistance the data protection officer needs. In turn, there is a recurring discussion item on the agenda for Samres Group’s executive management meetings called “report from Samres Data Protection Committee”, where the data protection officer is invited for discussions.

The Samres Group also has established legal contacts, such as law firms, which together form a competent network to which the data protection officer can turn for expert assistance.

14 AUDIT PROGRAM

14.1 The data protection officer has a duty to decide when the legal assistant shall conduct the internal data protection audits to ensure that the members of the Samres Group and their personnel comply with the provisions of the BCR-P. The audits take place in September or October each year. Additional audits can occur on the specific request of the data protection officer.

14.2 The internal data protection audits cover all aspects of the BCR-P, including methods of ensuring that corrective actions are taken if needed. These audits must, at least, include the following parts:

- Routines for informing personnel about updates of European Union or Member State data protection laws;
- Training programs used for educating personnel about data protection;
- Routines for managing requests from Data Subjects;
- Databases Processing Personal Data;
- Database applications used when Processing Personal Data;
- IT systems used when Processing Personal Data;
- Onward transfers of Personal Data to members of the Samres Group and external Sub-processors established outside the EEA;
- Company decisions taken regarding requirements under national laws that go against the BCR-P;
- Routines for informing personnel about updates in the BCR-P;
- Reviews of Data Processing Agreements, Processors and Sub-processors; and
- Corrective actions taken in response to Personal Data Breaches.

14.3 The results of the internal data protection audits are reported by the legal assistant to the data protection offices and the board of management of the Samres Group, who will, without undue delay, remedy any revealed data protection deficiencies.

14.4 The results of the internal data protection audit are also made accessible to the data controller and, upon request, to the Supervisory authority competent for that data controller.

14.5 The Processors and Sub-processors Processing Personal Data on behalf a Controller accept, at the request of the Controller, to submit their data Processing facilities to external data protection audits of any Processing activity related to that Controller. The audits are carried out by the Controller or an inspection body composed of independent members who are in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the Controller and, where applicable, in agreement with the competent Supervisory Authority.

14.6 The Supervisory Authority competent for the Controller can carry out external data protection audits of Processors and Sub-processors, if required.

15 THIRD PARTY BENEFICIARY RIGHTS

- 15.1 The Data Subjects have the right to enforce the following elements of the BCR-P as Third Party beneficiaries directly against the Processor where the requirements at stake are specifically directed to Processors in accordance with the GDPR. All GDPR Articles mentioned in this paragraph, BCR-P paragraph 15.1, can be found in Appendix 4:
- Duty to respect the Instructions from the Controller regarding Processing of Personal Data, including transfers of Personal Data to Third Countries (see Sections 1.3, 1.4, 8.1, 8.2 and 10 in the BCR-P and Articles 28.3.a, 28.3.g and 29 in the GDPR);
 - Duty to implement appropriate technical and organizational security measures (see Sections 10 and 11.1 in the BCR-P and Articles 28.3.c and 32 in the GDPR);
 - Duty to notify Personal Data Breaches to the Controller (see Section 10 in the BCR-P and Article 33.2 in the GDPR);
 - Duty to respect the data protection conditions when engaging a Sub-processor established within or outside the Group (see Section 6 in the BCR-P and Articles 28.2, 28.3.d, 28.4, 45, 46 and 47 in the GDPR);
 - Duty to cooperate with and assist the Controller in complying and demonstrating compliance with European Union or Member State data protection law, such as answering requests from Data Subjects in relation to their rights (see Sections 7.1, 7.2, 7.3, 10, 7.4, 8.1, 8.3, 8.4 and 8.5 in the BCR-P and Articles 28.3.e, 28.3.f and 28.3.h in the GDPR);
 - Right to easy access to the BCR-P (see Sections 5, 15.5 and 17.3 in the BCR-P and Article 47.2.g in the GDPR);
 - Right to complain through an internal complaint handling procedure (see Section 16 in the BCR-P and Article 47.2.i in the GDPR);
 - Duty to cooperate with the Supervisory Authority (see Section 7.5 in the BCR-P and Articles 31 and 47.2.l in the GDPR);
 - Duty to follow the liability, compensation and jurisdiction provisions (see Sections 15.1, 15.2, 15.3, 15.4, 15.5, 11.1 and 11.2 in the BCR-P and Articles 47.2.e, 79 and 82 in the GDPR); and
 - National legislation preventing respect of the BCR-P, see section 9 in the BCR-P (Article 47.2.m in the GDPR).

- 15.2 The Data Subjects have the right, in particular, to lodge a complaint to the competent Supervisory Authority of a Member State and the competent court of a Member State (in accordance with Article 79 in the GDPR, Article can be found in Appendix 4).
- 15.3 If Data Subjects cannot bring claims against the Controller, because that Controller has factually disappeared or ceased to exist in law or has become insolvent, they can enforce Sections 1.3, 15.1, 15.2, 15.3, 15.4, 11.1, 11.2, 5, 15.5, 16, 17.3, 7.5, 7.1, 8.1, 8.2, 7.2, 7.3, 10, 7.4, 6, 8.3, 8.4, 8.5, 1.1 and 9 in the BCR-P against the Processor. The Data Subjects cannot bring any claim against the Processor if a successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law, in which case the Data Subjects can enforce their Third Party beneficiary rights against that entity.
- 15.4 The Data Subjects are entitled to judicial remedies from the Processor for violations of the Third Party beneficiary rights guaranteed in Sections 15.1 and 15.3 in the BCR-P. The Data Subjects are also entitled to obtain redress and, where appropriate, receive compensation from the Processor for any damage (material harm but also any distress) caused by a violation of their Third Party beneficiary rights. If the Processor and the Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subjects are entitled to receive compensation for the entire damage directly from the Processor. The Processor can claim back from the Controller the part of the compensation that corresponds to the Controller's responsibility for the damage.
- 15.5 The Data Subjects benefiting from the Third Party beneficiary rights are in particular, provided with the information about their rights with regard to the Processing of their Personal Data and on the means of exercising those rights. It is the right of every Data Subject to have easy access to them. The entire BCR-P including appendices is, for that purpose, published on the official website of Samres.

16 COMPLAINT HANDLING PROCEDURE

- 16.1 The Samres Group offers a specific contact point for Data Subjects who wish to file a claim or request regarding the Processing of their Personal Data and in particular their Third Party beneficiary rights. The claim or request are sent by email to dpo@samres.se which is monitored by the data protection officer. Further instructions on how to file complaints or requests are published on the official website www.samres.se.
- 16.2 The members of the Samres Group have a duty to without undue delay communicate any claim or request from the Data Subjects to the Controller. The members of the

Samres Group are not obliged to answer the claim or request, unless they are authorized to do so by the Controller.

- 16.3 The Processors must handle requests from the Data Subjects if the Controller has disappeared factually, ceased to exist in law or become insolvent.
- 16.4 In all cases, where the Processors handle a complaint, they must handle it without undue delay and in any event within one month. Taking into account the complexity and the number of the requests, that period can be extended by two months at the utmost, in which case the Data Subjects must be informed about the fact of the delay and the reason of such delay within the same one month.
- 16.5 The Samres Group must notify, in writing, the Data Subjects of whether their claim or request is rejected or considered justified. The Samres Group must also inform the Data Subjects about their right to lodge a claim or request before the Supervisory Authority or the competent court of a Member State, if they regard the reply from The Samres Group as unsatisfactory, unduly delayed or indicative of a rejection. If the Samres Group finds the claim or request of the Data Subjects justified, it must make sure that corrective actions are taken by the relevant member of the Samres Group in order to ensure that Personal Data is Processed in accordance with the BCR-P.

17 UPDATES

- 17.1 Updates of the BCR-P are reported to the members of the Samres Group, to the competent Supervisory Authorities and to the controller. If an update affects the Processing conditions, information about that update must be given to the Controller in such a timely fashion that the Controller can object to the update or terminate the agreement before the update is implemented.
- 17.2 Updates of the BCR-P that adhere to the following provisions do not have to be re-submitted for approval by the Supervisory Authorities:
- The data protection officer must keep an updated list of the members of the Samres Group and external Sub-processors bound by the BCR-P involved in the Processing of Personal Data on behalf of the Controller and make that list accessible to the Controller, Data Subjects and relevant Supervisory Authorities;
 - The data protection officer must track and record any update of the BCR-P and systematically provide any necessary information about it to the Controller and, upon request, to the Supervisory Authorities;

- No transfer of Personal Data can be made to a new member of the Samres Group until the new member of the Samres Group has been effectively bound by the BCR-P and are able to deliver compliance;
- Updates of the BCR-P or the list of members of the Samres Group bound by the BCR-P must be reported once a year to the relevant Supervisory Authorities, via the competent Supervisory Authority, with a brief explanation justifying the updates; and
- If an update affects the level of protection offered by the BCR-P or significantly affects the BCR-P, it must be promptly communicated to the relevant Supervisory Authorities, via the competent Supervisory Authority.

17.3 The updated BCR-P and the list of members of the Samres Group and external Sub-processors bound by the BCR-P are published on the official website of Samres.

18 GOVERNING LAW

18.1 The BCR-P is, unless it indicates otherwise, governed by and construed in accordance with the laws of Sweden. In any event, Personal Data must be Processed in accordance with the applicable law. If Swedish legislation or any other local legislation requires a higher level of protection for Personal Data, it must nevertheless take precedence over the BCR-P.

19 INVALIDITY

19.1 In the event that any one or more of the provisions contained in the BCR-P will for any reason be held invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability will not affect any other provision of the BCR-P.

The BCR-P has been duly executed in four (4) original copies, of which each of the members of the Samres Group has taken one copy.

[Place, date]

Samres AB

Samreis Eesti AS

[Authorized signatory]

[Authorized signatory]

[Authorized signatory]

[Authorized signatory]

Samres South East SRL

Samres Senegal SUARL

[Authorized signatory]

[Authorized signatory]

[Authorized signatory]

[Authorized signatory]