Calea Plevnei 159,
Business Garden Bucharest,
Building C, 4th floor, Bucharest
+ 40 (21) 212 26 69
osf.digital

OSF Binding Corporate Rules

Contents

1. INTRODUCTION

OSF Global Services was founded in 2003, in Québec City, Canada with additional operations taking place in Bucharest, Romania.

OSF employee count exceeds 1000, with many employees taking advantage of distributed work environment. OSF is headquartered in Québec, Canada, and also has offices in the U.S., UK, France, Germany, Brazil, Spain, Romania, Ukraine, Colombia, and Japan, among many other locations worldwide.

OSF Global Services is a leading global commerce and digital cloud transformation company, with expertise in enterprise CRM, CMS, OMS, connected commerce, online shop management and cloud application development. OSF agile approach allows to scale global growth more quickly, and to deliver innovative solutions across channels, devices and locales to enterprises and emerging businesses across B2B and B2C sectors. Winner of the 2019 Bolty Award for Best Digital Experience in the Retail and Consumer Goods category, the 2019 Partner Innovation Award in the Customer 360 category, and the 2018 Salesforce Lightning Bolt Trailblazer Award for Retail, OSF guides businesses throughout their end-to-end digital journey, starting with consulting, strategy planning, implementation, integration and optimization, through to training, support and maintenance. HSBC and BDC are OSF's main financial partners, and Salesforce Ventures and Delta-v Capital are OSF's investors.

OSF Global Services Inc. and its affiliates (hereinafter "OSF Entities", or "OSF" or "OSF Entity") are committed to achieving and maintaining customer trust. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters.

These binding corporate rules express OSF's commitment to protect personal data that OSF Entities process while operating their business and to ensure adequate safeguards for transfers of personal data outside EU/EEA, in accordance with the 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 ("GDPR" or "General Data Protection Regulation") and data protection legislation of the relevant countries.

2. DEFINITIONS

a. **Applicable Data Protection Law** means General Data Protection Regulation and any other laws applicable to the Processing of Personal Data in the EU member states/EEA countries, including the laws implementing GDPR.
b. **Binding Corporate Rules (BCR or BCRs)** means the data protection policies adhered to by companies established in the EU/EEA for transfers of Personal Data outside the EU/EEA within a group of undertakings or enterprises.
c. **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her; **Explicit consent** refers to the way consent is expressed by the data subject, respectively it means that the data subject must give an express statement of consent;

d. **Controller** means the entity established in the EU/EEA and not a member of the OSF group, which determines the purposes and the means of the processing of Personal Data; For the scope of these BCRs, the Customer acts as Controller.

e. **Customer** means (i) a legal entity with whom an OSF Entity has executed a contract to provide the Services (or a legal entity placing an order under such contract), contract that incorporates by reference OSF Processor BCRs or (ii) a legal entity with whom an OSF Entity has executed a contract entitling that legal entity to resell OSF Services to its end customers, contract that incorporates by reference OSF Processor BCRs.

f. **Data Processing Addendum and Annexes (DPAA)** - provides a set of additional obligations regarding the Processing of Personal Data according to GDPR, that OSF undertakes as part of an agreement (MSA/SOW) with each Customer.

g. **Data Subject** means the identified or identifiable natural person to whom Personal Data relates.

h. **EEA** means the European Economic Area, which consist of European Union member states, as well as Norway, Iceland and Liechtenstein.

i. **Employee** means any person who is hired by OSF or independent contractor to whom applies all OSF's employment policies and procedures (OSF credentials management of internal systems, employees' management, etc) and who is bound to respect these BCRs.

j. **EU OSF Delegated Entity** means the EU headquarters of OSF and member of these BCRs, that accepts responsibility for and agrees to take the necessary action to remedy the acts of other OSF Entity established outside of EU/EEA or breaches caused by External Sub-Processor established outside of EU/EEA and to pay compensation for any damages resulting from a violation of the OSF BCR. For the scope of these BCRs, the EU OSF delegated Entity is **S.C. OSF Global Services S.R.L. Romania**.

k. **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

l. **Intra Company Agreement** – a document that makes OSF BCR binding among all OSF Entities.

m. **International Data Transfer** means the transfer of Personal Data from the Controller in the EU/EEA to the Processors and/or Sub-Processors in a Third Country, as well as the transfer of Personal Data from the Processor in the EU/EEA to Sub-Processors/External Sub-Processors in a Third Country.

n. **Master Service Agreement** (MSA) means a contract concluded between an OSF Entity and a Customer, including a common set of legal, commercial and confidentiality terms that will govern most of future Statements of Work in order to speed up and simplify future contracts between the parties. OSF BCR will be made enforceable for the Customer/Controller through a specific reference to it in the MSA - as an annex.

o. **OSF** or **OSF Entity** (or plural, **OSF Entities**) means the OSF Global Services, Inc. a company incorporated in Canada, and any and all OSF affiliates stated in Annex 2 to these BCRs – their locations being detailed on OSF's website, available at https://osf.digital/contact-us.

p. **OSF BCR** or **OSF Processor BCRs** means these Binding Corporate Rules for the Processing of Personal Data applicable to any and all OSF Entities.

q. **Personal Data** means any information relating to a Data Subject 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.

r. **Personal Data Breach** means 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** has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly. Processing means 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.

s. **Processor** means the entity acting on behalf of the controller; For the scope of these BCRs, OSF acts as a Processor.

t. **Sensitive Personal Data** refers to specific categories of Personal Data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

u. **Services** means the services provided to Customer by an OSF Entity pursuant to the MSA and/or SOW, as listed in Annex 3.

v. **Sub-Processor** might be either an OSF Entity or a third party that is not an OSF Entity, such as a contracting partner of the Processor (**External Sub-Processor**), that processes Personal Data of the Data Subject that were sent to the Processor in order to perform the Services making the object of the contract concluded with the Customer.

w. **Supervisory Authority** means independent public authority which is established by a member state pursuant to Article 51 of GDPR; **Lead Supervisory Authority** means the supervisory authority of the establishment of the EU OSF Delegated Entity, with the primary responsibility for dealing with cross-border processing activity regarding these BCRs, which is the **Romanian Supervisory Authority** (in Romanian, "Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal"/"ANSPDCP");

x. **Statement of Work (SOW)** means a contract between any OSF Entity and the Customer which either states a detailed, fixed scope of activities, functionality, and delivery timeline(s) the OSF Entity must comply with or defines the type, number of resources the OSF Entity must make available for the Customer. The SOW also includes detailed customer requirements and deliverables, price and payment terms, and may include special regulatory and governance terms and conditions that may amend the general terms included in the Master Services Agreement

y. **Third Country** means any country other than the Member States of the European Union/EU and the three additional countries of the European Economic Area/EEA (Iceland, Norway, and Liechtenstein) that have adopted a national law implementing the GDPR.

3. OSF BCR APPLICATION & SCOPE

3.1 Material Scope

OSF Processor BCRs apply to the OSF Entities which have signed an Intra Company Agreement regarding the Processing of Personal Data in respect of which an OSF Entity has a signed contract (e.g. MSA, SOW or DPAA) with the relevant Customer acting as Controller.

A list of OSF Entities members of these OSF Processor BCRs (including contact details) is attached as Annex 2 and available online here.

The purpose of the OSF BCR is to govern cross-border transfers of Personal Data to and between OSF Entities and to External Sub-Processors (in accordance with written agreements with any such External Sub-Processors), when OSF acts as Processor or Sub-Processor, on behalf and under the documented instructions of a Customer as Controller.

The OSF Processor BCRs apply to Personal Data provided in connection with the Services by:

(a) Customers established in EEA member states whose processing activities for the relevant data are governed by GDPR and implementing national legislation; and

(b) Customers established in non-EEA member states for which the Customer has contractually specified that GDPR and implementing national legislation shall apply.

OSF shall make the OSF Processor BCRs, including the members of the OSF, available at https://osf.digital/company/compliance.

The following categories of Personal Data are processed when OSF provides Services to its Customers:

- Identification data of Customer's representatives and contact persons: name, surname, company, department, title, position, business email & phone, business address.
- Identification data of Customer's clients - individuals: personal email address, work email address, name, surname, name of employer, client profile picture, work phone number, personal phone number, work location, personal address, user name, password, orders from e-commerce website, credit card information, gender, age, financial data, national ID data, IP location, native language, known languages, browser user agent, Facebook ID, Google ID, user generated content: social media content, messages, work related tracking data, geolocation tracking data.

If the processing of Sensitive Personal Data is required for the provision of Services by OSF, the specifications of Section 10 below are applicable. Categories of Data Subjects to which the Personal Data relates:

- Customers or prospective Customers.
- Employees, representatives or other personnel having a contractual relation with the Customer or prospective Customer.
- Customers 'clients - individuals or prospective Customers 'clients-individuals.

3.2 Geographical Scope

OSF BCR applies to all OSF Entities, as described in Annex 2 of these BCRs, regardless of their localization and legal jurisdiction.

The geographical scope of the OSF BCR is comprised of all EU/EEA countries as well as any other non-EU/EEA countries in which OSF Entities are present.

Where an OSF Entity acts as a Processor or Sub-Processor, it shall be the responsibility of the Customer acting as Controller to determine whether to apply the OSF Processor BCRs to:

- all Personal Data processed for processor activities and that are submitted to the EU/EEA law (e.g. Personal Data that is transferred from the EU/EEA); or
- all Personal Data for processor activities, irrespective of the data's origin.

3.3 The duty to observe the OSF BCR for OSF Entities and their Employees

To secure the binding nature of the OSF BCR, OSF Entities conclude an Intra Company Agreement that incorporates also the OSF Processor BCRs. OSF Processor BCRs are legally binding for each and all OSF Entities and each OSF Entity stated in Annex 2 to these BCRs. OSF commits to keep this list up-to-date and to communicate it on request to the relevant parties.

Each and all OSF Entities, as well as their Employees shall respect the OSF BCR, as well as the documented instructions from the Customer, as Controller, regarding the Processing as well as the security and confidentiality measures as provided in the contract concluded between the OSF Entity and that Customer in fully compliance with Articles 28, 29 and 32 of the GDPR.

OSF BCR are included in the OSF Group policies which Employees are bound to respect according to their job description responsibilities.

4. PRINCIPLES FOR PROCESSING PERSONAL DATA

When Processing Personal Data, OSF guarantees that the following principles for Processing Personal Data are observed:

i. Transparency, fairness and lawfulness

Processors and Sub-Processors have a general duty to assist the Controller to comply with the law, including assistance to be transparent about sub-processor activities in order to allow the Controller to correctly inform the Data Subjects.

ii. The purpose of the Processing is determined, explicit and legitimate ("purpose limitation")

Processors and Sub-Processors shall process Personal Data only in accordance with the MSA, SOW or DPAA concluded, and otherwise in accordance with the Customer's documented instructions. More specifically, OSF shall process Personal Data on behalf of the Customer as Controller:

- for the sole purposes prescribed by the Customer, and
- in accordance with the conditions set forth in the MSA, SOW or DPAA document concluded between OSF and the respective Customer.

If OSF cannot comply with such purpose limitation, OSF shall promptly notify the Customer, which shall be entitled to suspend the transfer of Personal Data and/or terminate the applicable SOW only for those Services that cannot be provided by the OSF in accordance with Customer's instructions.

Also, OSF shall immediately inform the Customer if, in its opinion, an instruction of the Controller infringes the Applicable Data Protection Law and will stop that processing until the situation is remediated or clarified.

At the termination of the contract with the Controller, Processors and Sub-Processors shall, based on the documented instructions of the Controller, return all the Personal Data transferred and the copies to the Controller or shall destroy all the Personal Data and certify to the Controller that it has done so, unless law imposed upon them prevents it from returning or destroying all or part of the Personal Data. In such case, the Processors and Sub-Processors will inform the Controller and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

iii. The Personal Data processed are relevant and not excessive ("data minimization") and are not stored longer than necessary ("storage limitation")

Personal Data processed by Processors and Sub-Processors will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Processors and Sub-Processors will keep Personal Data in a form which permits identification of Data Subjects, for no longer than is necessary for the purposes for which the Personal Data is processed.

The purposes of retaining the Personal Data, and the specific retention periods, will be as instructed by the Controller or, in the absence of any such instructions, in accordance with OSF's applicable policies/procedures.

OSF's storage periods are determined by factors such as the need to retain data to provide services to Data Subjects or Customers, the need to comply with applicable laws.

OSF limits access to Personal Data to those personnel who need access to the data to fulfil their responsibilities. OSF personnel with access to Personal Data are forbidden from accessing or using this data for other reasons than fulfilling their duties. OSF requires External Sub-Processors to adopt a similar approach to Personal Data they access in connection with providing services to OSF.

iv. The Personal Data are kept accurate and updated ("accuracy")

In accordance with the request from the Controller, Processors and Sub-Processors will take every reasonable step to ensure that, in relation to the purposes for which it is processed, Personal Data that is inaccurate is erased or rectified without delay and will inform any other OSF Entity to whom it has disclosed such Personal Data of such erasure or rectification, if applicable. Processors and Sub-Processors will execute any

necessary measures, when asked by the Controller, in order to have the Personal Data deleted or anonymized from the moment the identification form is not necessary anymore. Processors and Sub-Processors will communicate to each entity to whom the data has been disclosed of any deletion or anonymization of Personal Data.

v. The appropriate security measures are implemented according to OSF security policy ("integrity and confidentiality")

Processors and Sub-Processors implement appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss or destruction. OSF regularly reviews and, as appropriate, enhances its security systems, in line with technical developments.

Personal Data will not be transferred to a Third Country or international organization which has inadequate data protection laws, unless adequate safeguards are in place according to GDPR provisions, as described in Section 11 below.

Processors and Sub-Processors shall assist the Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR considering the nature of processing Personal Data and information available to the Processor.

5. OSF RESPONSIBILITY

OSF BCR are available to Data Subjects, Controllers and OSF Employees on _____ website.

5.1 OSF's responsibility towards the Customer as Controller

i. Responsibility towards the Controller: When an OSF Entity acts as a Processor for a Customer, OSF makes specific reference in the MSA, SOW and/or DPAA to the binding character of these BCRs - as an annex, which shall comply with Article 28 of the GDPR.

The Controller has the right to enforce the OSF Processor BCRs against any OSF Entity for breaches they caused, and, moreover, against the EU OSF Delegated Entity in case of a breach of these BCRs or of the MSA/SOW/DPAA by OSF Entities established outside of EU/EEA or the written agreement referred under Section 11 below, by any External Sub-Processor established outside of the EU/EEA.

ii. Record keeping: In order to demonstrate compliance with the OSF Processor BCRs, OSF shall maintain a record of all categories of processing activities carried out on behalf of the Controller, containing:

a) the name and contact details of the Processor and of the Controller on behalf of which OSF Entity is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer.
b) the purposes of the Processing.
c) a description of the categories of Data Subjects and of the categories of Personal Data processed on behalf of the Controller.
d) the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in Third Countries or international organizations.

e) where applicable, transfers of Personal Data to a Third Country or international organization, including the identification of that Third Country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards.
f) where possible, the envisaged time limits for erasure of the different categories of Personal Data.
g) where possible, a general description of the technical and organizational measures referred to in Article 32(1) of the GDPR.

The records of data processing activities carried out on behalf of the Controller shall be in writing, including in electronic form.

OSF shall make the data processing record available to the Supervisory Authority on request.

iii. Cooperation with the Controller: OSF undertakes the obligation to cooperate to the extent reasonably possible and assist the Controller to comply with the Applicable Data Protection Law (e.g. the obligation to respect the Data Subject rights and to handle the complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities).

OSF makes available to the Customer acting as Controller all information necessary to demonstrate compliance with its obligations as provided by Article 28 (3) letter h) of the GDPR, and allows for and contributes to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, as described in the Section 9.2 below.

iv. Data Subject Rights: Customer acting as Controller has primary responsibility for interacting with Data Subjects. OSF shall execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the Controller, for the fulfilment of the Controller's obligations to respond to requests for exercising the Data Subjects rights as set out in Chapter III of the GDPR, including by communicating any useful information in order to help the Controller to comply with its duty to observe the Data Subjects rights.

OSF acts in accordance with the terms of the MSA, SOW and/or DPAA concluded with the Customer acting as Controller and undertakes any reasonably necessary measures to enable the Controller to comply with its duties to respect the rights of Data Subjects according to GDPR provisions.

OSF shall promptly notify the relevant Controller if it receives a request from a Data Subject for access to, correction, amendment or deletion of that Data Subject's Personal Data.

OSF handles requests from Data Subjects in accordance with the Controller's instructions included in the MSA, SOW or DPAA that it has concluded with that Controller, which may include transferring the request to the relevant Controller and not responding to such request, and — where applicable — the Data Subject Access Request Procedure as set out in Annex 5 to these BCRs.

5.2 Cooperation with the Supervisory Authorities

OSF will cooperate with the Supervisory Authorities in relation to these BCRs. Where required, OSF will be available to discuss with the Supervisory Authorities in relation to these BCRs.

All OSF Entities have the duty to cooperate with the Supervisory Authorities competent for the relevant Controller and to comply with the advice of these Supervisory Authorities on any issue related to the OSF Processor BCRs.

Upon request and subject to the confidentiality obligations, OSF shall provide the Supervisory Authority competent for the relevant Controller a copy of OSF BCR and/or other requested documentation and will allow the onsite audit of OSF architecture, systems and procedures relevant to the protection of Personal Data.

OSF will consider:

- the views and guidelines of the European Data Protection Board and Article 29 Working Party on Binding Corporate Rules for Processors,
- decisions made by the Supervisory Authorities on any data protection law issues that may affect these BCRs.

Upon request, OSF will provide copies of the results of any assessment of compliance of these BCRs to the Supervisory Authority competent for the Controller, subject to the applicable law and observance of the confidentiality principles. OSF shall cooperate to handle a request or complaint from an individual or an inquiry from the Supervisory Authorities.

Also, OSF shall cooperate actively with the Supervisory Authorities to ensure adequate and timely response to any inquiry received.

6. THIRD-PARTY BENEFICIARY RIGHTS

6.1(a) Rights which are directly enforceable against the Processor

Data Subjects are entitled to enforce the following provisions of the OSF Processor BCRs as third-party beneficiaries directly against OSF as Processor where the requirements at stake are specifically directed to Processors in accordance with the GDPR:

i. Duty to observe the OSF Processor BCRs, as well as to comply with the instructions from the Controller regarding the Processing, including for data transfers to Third Countries (Sections 3.1 and 3.3, Section 4, Sections 8.2 and 8.3, Section 10, Section 11)

ii. Duty to implement technical and organizational measures, and duty to notify any security data breach to the Controller (Section 4 (v), Sections 8.2 and 8.3)

iii. Duty to respect the conditions when engaging a Sub-Processor either within or outside OSF (Sections 7 and 11)

iv. Duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation

to their rights (Section 4, Section 5.1 and by extension Annex 5, Sections 8.2 and 8.3, Section 9.2, Section 12 and Section 13)

v. Easy access to OSF BCR (Section 6.3)

vi. Right to complain through internal complaint mechanisms (Section 6.2, and by extension Annex 6)

vii. Duty to cooperate with the Supervisory Authority (Section 5.2, Section 16)

viii. Liability of OSF. Burden of proof. Compensation and jurisdiction (Section 6.4)

ix. Local law requirements. Requests from public authorities (Section 6.5)

x. Third-Party Beneficiary Rights (Section 6)

6.1(b) Rights which are enforceable against the Processor in case the Data Subject is not able to bring a claim against the Controller

Where Data Subjects are not able to bring a claim against the Controller, respectively in case that the Controller has factually disappeared or ceased to exist in law or has become insolvent and that no other entity has assumed the legal obligations of the Controller (in which case the Data Subject can enforce its rights against such entity), Data Subjects shall at least be able to enforce the following provisions of OSF Processor BCRs as third-party beneficiaries against OSF as Processor:

i. Duty to respect the OSF Processor BCRs (Sections 3.1 and 3.3)
ii. Responsibility towards the Controller (Section 5.1.i)
iii. Liability of OSF. Burden of proof. Compensation and jurisdiction (Section 6.4)
iv. Local law requirements. Requests from public authorities (Section 6.5)
v. Easy access to OSF BCR (Section 6.3)
vi. Right to complain through internal complaint mechanisms (Section 6.2, and by extension Annex 6)
vii. Duty to cooperate with the Supervisory Authority (Section 5.2, Section 16)
viii. Duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Section 4, Section 5.1 and by extension Annex 5, Sections 8.2 and 8.3, Section 9.2, Section 12 and Section 13)
ix. Privacy principles including the rules on transfers or onward transfers outside of the EU/EEA (Section 4, Section 5.1.iv, Section 10, Sections 8.2 and 8.3, Sections 7 and 11)
x. Accountability principle and other tools under GDPR (Section 4. ii, Section 5.1.ii, Sections 12 and 13)
xi. List of the OSF Entities bound by the OSF BCR mentioning their contact details is included in the OSF BCR (i.e. Annex 2 to the OSF BCR)
xii. Third-Party Beneficiary Rights (Section 6)

6.2 Right to complain through internal complaint mechanisms

Data Subjects may lodge a complaint related to the Processing of their Personal Data carried out by OSF under the OSF Processor BCRs, by sending an email at: dataprotection@osf.digital.

All OSF Entities shall have the duty to communicate without undue delay a Data subject's claim or request to the Customer/Controller without obligation to handle it (except if it has been agreed otherwise with the Controller).

All complaints regarding Processing of Personal Data carried out by OSF on behalf of Controllers will be handled by observing the provisions of Annex 6 - Complaint Handling Procedure.

Where OSF is aware of the fact that a Customer has disappeared factually or has ceased to exist in law or become insolvent, it undertakes to handle the Data Subjects' complaints.

In all cases where OSF, as Processor, handles Data Subjects' complaints, these shall be dealt without undue delay and in any event within one month of receipt of that complaint. Considering the complexity and number of the requests, that period of one month may be extended by two further months at the utmost, in which case the Data Subject will be informed accordingly.

If Data Subject is not satisfied with the way in which the complaint in question has been resolved by OSF, Data Subject has the right to lodge a complaint before the court or with a Supervisory Authority.

6.3 Transparency and easy access to OSF BCR

Access for the Controller: When an OSF Entity acts as a Processor for a Customer, OSF makes specific reference in the MSA/SOW/DPAA to the binding character of these BCRs, with a possibility of electronic access, or OSF Processor BCRs are annexed to the respective MSA/SOW/DPAA.

Access for the Data Subject: All Data Subjects benefiting from the third-party beneficiary rights have the right to be provided with the information on their third-party beneficiary rights with regard to the processing of their Personal Data and on the means to exercise those rights.

Data Subjects may obtain a copy of the OSF Processor BCRs from the OSF Entity responsible for exporting the data outside EU/EEA or any other OSF Entity, or by accessing the OSF Processor BCRs published on the OSF's website at https://osf.digital/company/compliance.

6.4 Liability of OSF. Burden of proof. Compensation and jurisdiction

i. Liability of OSF: In case of a breach of OSF Processor BCRs by an OSF Entity established outside of EU/EEA, or by an External Sub-Processor established outside of EU/EEA, OSF Global Services SRL Romania, as the EU OSF Delegated Entity, will be liable for and will take all the required actions to remedy any such acts and to pay compensation for any damages resulting from a violation of the OSF Processor BCRs.

The EU OSF Delegated Entity shall be liable for the breach or action of the OSF non-EU/EEA Entity as if the violation had taken place by EU OSF delegated Entity in the member state in which this entity is based instead of the OSF non-EU/EEA Entity or OSF external non-EU/EEA Sub-Processor, and may not rely on a breach by a Sub-Processor (either an OSF Entity or an External Sub-Processor) of its obligations in order to avoid its own liabilities.

ii. Burden of proof:

To the extent a Controller (or a Data Subject) demonstrates that they have suffered damage and establishes facts showing that the damage has likely occurred because of the breach of the OSF BCR by an OSF Entity or any External Sub-Processor established outside the EU/EEA, the EU OSF Delegated Entity has the burden of proof to demonstrate that such OSF Entity or such External Sub-Processor is not responsible for the breach of the OSF BCR giving rise to the respective damage or that no such breach took place.

For more clarity, the burden of proof will be reversed so that, rather than it being the responsibility of the individual making a claim to show that an OSF Entity or any External Sub-Processor established outside EU/EEA is liable for the breach or that such a breach took place, it will be for the EU OSF Delegated Entity to prove that the OSF Entity or the respective External Sub-Processor established outside EU/EEA is not liable for the breach, or that such breach did not occur.

If the EU OSF Delegated Entity can prove that the OSF Entity or External Sub-Processor established outside the EU/EEA is not responsible for the event giving rise to the damage, it may discharge itself from any liability/responsibility.

iii. Compensation: The Data Subjects' rights as mentioned under Sections 6.1(a) and 6.1 (b) cover judicial remedies for any breach of the third-party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress).

Where the Processor and the Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from OSF acting as Processor or from the Controller.

iv. Jurisdiction: Data Subjects are entitled to lodge a complaint with the competent Supervisory Authority (choice between the Supervisory Authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement) and before the competent court of the EU Member State (choice for the Data Subject to act before the courts where the Controller or Processor has an establishment or where the Data Subject has his or her habitual residence).

6.5 Local law requirements. Requests from public authorities

i. Local law preventing OSF from complying with the OSF BCR: Where an OSF Entity has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller or its obligations under the OSF Processor BCRs or Master Service Agreement, it will promptly notify this

to the Controller which is entitled to suspend the transfer of data and/or terminate the contract, to the EU headquarter Processor or EU OSF Delegated Entity or the other relevant privacy officer/function, but also to the Supervisory Authority competent for the Controller and the Supervisory Authority competent for the Processor.

ii. Relationship between local law and OSF BCR: Where the data protection law applicable within the relevant EU/EEA Member State requires a higher level of protection for Personal Data than provided for in the OSF BCR, that law shall take precedence.

iii. Requests from public authorities: Any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body (the "Request") shall be communicated to the Controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). Thus, if OSF receives a Request, the person receiving the Request must pass it to OSF 's data protection officer immediately upon receipt, indicating the date on which it was received and any other relevant information.

In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the Controller and the competent Supervisory Authority for the Processor should be clearly informed about such request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited). If in specific cases the suspension and/or notification are prohibited, the requested OSF Entity will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested OSF Entity is not in a position to notify the competent Supervisory Authorities, it shall annually provide general information on the requests it received to the competent Supervisory Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

Where an OSF Entity will provide Personal Data to a public authority, such data provision will not involve a massive or disproportionate amount of Personal Data, nor will it be discriminatory in such a way as to go beyond what is necessary in a democratic society.

OSF keeps a written record of all the Requests and procedure followed.

7. SUB-PROCESSING OPERATIONS

7.1 Commitments concerning Sub-Processors

Personal Data may be processed by Sub-Processors, respectively by other OSF Entities or by External Sub -Processors, only with prior information of the Controller and its prior specific or general written authorization as provided under the terms of the MSA, SOW and/or DPAA concluded between respective Controller and OSF Entity, as Processor.

If a general authorization is given, OSF shall inform the Controller of any intended changes concerning the addition or replacement of a Sub-Processor in such a timely fashion that the Controller has the possibility to object to the change or to terminate the contract before any transfer of Personal Data to the new Sub-Processor, as described in the Section 7.2.C below.

OSF ensures that any Sub-Processor, whether External Sub-Processor or an OSF Entity is bound by a written agreement compliant with and including all required elements provided by Article 28(3) of the GDPR. Thus, where a Sub-Processor has access to Personal Data processed by OSF acting as Processor, OSF imposes strict contractual obligations regarding:

i. the security of such Personal Data, consistent with those contained in the OSF Processor BCRs and with the terms of MSA, SOW and/or DPAA that OSF has concluded with the Customer,
ii. the Sub-Processor's obligation to act only on OSF's instructions when using Personal Data processed by OSF acting as Processor, as well as
iii. the Sub-Processor's obligation to notify OSF without undue delay after becoming aware of any Personal Data breach.

OSF will ensure that Sub-Processors undertake to comply with provisions that are consistent with the terms in the MSA, SOW and/or DPAA concluded by OSF with the Customer, as Controller.

7.2. Description of Sub-Processing

A. Sub-Processing within OSF

As set forth in the applicable MSA, SOW or DPAA concluded by OSF with the Customer, OSF Entities may act as Sub-Processors of Personal Data, and depending on the location of the OSF Entity, processing of Personal Data by such Sub-Processors may involve transfers of Personal Data. This Section 7.2.A is complemented by provisions of Section 11 below. OSF Processor BCRs cover any and all OSF Entities as detailed above.

B. Sub-Processing by third parties

OSF may engage third-party Sub-Processors (i.e. External Sub-Processors) based on prior general or specific written authorization of the Controller, as set forth in the applicable MSA, SOW or DPAA concluded between OSF and the Customer. Depending on the location of the External Sub-Processor, Processing of Personal Data by such Sub-Processors may involve transfers of Personal Data. This Section 7.2.B is complemented by provisions of Section 11 below.

The current list of third-party Sub-Processors Processing Personal Data, including a description of their processing activities, is available here.

C. Notification on new Sub-Processors and objection rights

OSF may, by giving no less than thirty (30) days' notice to Customer/Controller, add or make changes to the Sub-Processors list.

If, once provided with the list of OSF's Sub-Processors, Customer objects to the appointment of an additional Sub-Processor within fourteen (14) days of such notice on reasonable grounds related to the protection of the Personal Data, OSF shall have- at its sole discretion- the following options:

(a) to provide the Services without the Sub-Processor that was rejected by the Customer; or

(b) to take the corrective steps requested by Customer/Controller in relation with the Sub-Processor in order to use that Sub-Processor; or

(c) to cease (temporarily or permanently) the provision of the Services that would involve the use of such Sub-Processor.

Any objections regarding a Sub-Processor shall be submitted to OSF to: legal@osf.digital.

If the Customer's objection cannot be solved by the parties within 30 (thirty) days, any party is entitled to terminate the MSA/SOW/DPAA concluded between OSF and Customer.

D. Emergency replacement

In emergency cases when the provision of Services is subject to replacement of a specific Sub-Processor, OSF may replace a Sub-Processor if the reason for the change is beyond OSF's reasonable control. In such a case, OSF shall notify the Customer about the replacement of the respective Sub-Processor as soon as reasonably practicable, and the Customer shall have the right to object to the replacement of that Sub-Processor pursuant to the Section 7.2.C above. The relevant provisions mentioned above shall be applicable.

E. Breach by a Sub-Processor

OSF shall remain liable for any breach of the data protection obligations caused by a Sub-Processor.

8. CONFIDENTIALITY AND SECURITY MEASURES

8.1 Confidentiality and Training

OSF trains its Employees on the basic principles of data protection, confidentiality and information security awareness. Training and awareness will be provided periodically, through a yearly training and evaluation of the knowledge achieved. Updates regarding GDPR related subjects are included in the yearly data protection training. All updates and messages related to GDPR updates are announced via OSF Community portal.

OSF shall ensure that its Employees engaged in the processing of Personal Data are informed of the confidential nature of the Personal Data, have executed written confidentiality agreements and have received appropriate training on their responsibilities.

Additionally, OSF shall ensure that its Employees responsible for the development of tools used to process Personal Data have received appropriate training on their

responsibilities. OSF shall also ensure that its Employees engaged in the processing of Personal Data are limited to those personnel who require such access to perform the OSF's obligations under MSA or SOW and/or DPAA concluded by OSF with the Customer. New hires are required to complete the training as part of their induction program.

OSF Processor BCRs are enforceable and effective throughout the OSF group, being obligatory for each and every OSF Entity and its Employees.

OSF commits to and implements:

- A comprehensive OSF global security and data protection training program
- Provide required training to all Employees.

OSF Data Protection Officer has overall responsibility for privacy and data protection training at OSF, with the colleagues' input from other functional areas within OSF, including the Information Security, Human Resources, as appropriate. OSF will review the privacy and data protection training from time to time to ensure it addresses all relevant aspects of the OSF global security and privacy policy and that it is appropriate for the Employees who have permanent or regular access to Personal Data, and who are involved in the processing of Personal Data.

Communication and training will cover data privacy elements such as: data protection principles, definitions, data privacy considerations with respect to information security, etc.

The attendance to the OSF global security and data protection training program will be monitored by the Data Protection Officer together with the Quality Management department and IT Security Manager.

OSF will regularly provide reinforcement content to OSF personnel regarding their responsibilities on data protection, confidentiality and information security awareness. Such content will be provided via OSF's Intranet.

8.2 Data Security

Processors and Sub-Processors have the duty to implement technical and organizational measures which at least meet the requirements of the Controller's applicable law and any existing measures specified in the MSA, SOW and/or DPAA signed with the Customer, as Controller.

OSF adheres to IT security policies and the information security measures as specified in the MSA, SOW and/or DPAA concluded by OSF with a Controller.

OSF maintains appropriate administrative, technical and physical safeguards for protection of the security, confidentiality and integrity of Personal Data, as set forth in applicable contracts with Customers. OSF regularly monitors compliance with these safeguards. OSF will not materially decrease the overall security of the Services during a Customer's applicable subscription term.

OSF complies with the requirements contained in the OSF security policies as revised and updated from time to time together with any other information security procedures relevant to a business area, as well as with information security measures according

to GDPR provisions and specified in a MSA, SOW and/or DPAA concluded by OSF with a Customer.

Processors and Sub-Processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the Customer acting as Controller, for the fulfilment of the Controller's obligations to respond to requests for exercising the Data Subjects rights as set out in the GDPR, including by communicating any useful information in order to help the Controller to comply with the duty to respect the rights of the Data Subjects, as mentioned in the Section 5.1 above.

8.3 Notification of Personal Data Breach

In the event that OSF becomes aware of any unauthorized access to or disclosure of Personal Data, OSF will notify without undue delay the affected Customers acting as Controllers to the extent required by the Applicable Data Protection legislation and in accordance with the terms of the MSA, SOW and/or DPAA concluded by OSF with the relevant Controllers.

Also, the External Sub-Processors will be bound by contract to inform the Processor and the Controller without undue delay after becoming aware of any Personal Data Breach.

9. DATA PROTECTION AUDITS

OSF shall maintain an audit program to help ensure compliance with the OSF Processor BCRs, internal verification and audits by Customers. The audit program covers all aspects of the OSF BCR, including methods for ensuring compliance.

The audits shall be carried out on a regular basis, with no more than 3 years between each audit. Such an audit shall be carried out by the OSF internal audit team and the audit reports shall be presented to the OSF Board.

The results of the audit shall be communicated to the Compliance team (including Top Management) and corrective actions shall be proposed, if may be the case. The results of such an audit will also be made accessible to the Controller, based on the latter's request.

Upon request, the Supervisory Authorities competent for the Controller may have access to the results of the data protection audit. Also, the Supervisory Authorities are entitled to carry out a data protection audit of any OSF Entity, if required.

The Controller can request an audit to be carried out at OSF and/or at Sub-Processors' facilities used to process Controller's Personal Data. Such audit request shall be performed only with the prior notification of OSF.

The audit plan dedicated to these BCRs is described in Annex 8.

9.1 Internal Verification

OSF has appointed a compliance team responsible for overseeing and ensuring conformity with OSF data protection responsibilities at a local and global level, including compliance with the OSF BCR, advising management on data protection matters, liaising with Supervisory Authorities, and handling data protection-related complaints.

OSF compliance department shall conduct a periodical (e.g. annually) assessment of OSF compliance with OSF BCR, which is provided to OSF appointed IT Security Manager, Data Protection Officer and OSF board of directors. Such an assessment shall include any necessary corrective actions, timeframes for completing such corrective actions, and follow up by OSF compliance department to ensure such corrective actions have been completed.

9.2 Customer Audits

Upon a Customer's request and subject to appropriate confidentiality obligations, OSF shall make available to the Customer (or such Customer's independent, third-party auditor that is not a competitor of OSF) information regarding OSF and third-party sub-processors' compliance with the data protection controls set forth in these OSF Processor BCRs. This includes providing the requesting Customer a report of OSF audits of third-party sub- processors, which the Customer instructs OSF to conduct as per MSA, SOW and/or DPAA signed by OSF with a Customer, according to GDPR provisions.

The Customer (or such Customer's independent, third-party auditor that is not a competitor of OSF) may also request to conduct an on-site audit of the architecture, systems and procedures relevant to the protection of Personal Data at the locations where Personal Data is stored, or an inspection, including at OSF Entities and third-party sub-processors' locations, by following the instructions set forth in MSA, SOW and/or DPAA. The requesting Customer will reimburse OSF for any time spent by OSF or its third-party sub-processors for such on-site audit at OSF, at the current professional service rates, which shall be made available to the Customer upon its request.

Before any such on-site audit, the requesting Customer and OSF shall mutually agree upon the scope, timing, and duration of the audit as well as on the reimbursement rate to be paid by the Customer. All reimbursement rates shall be reasonable, considering the resources spent by OSF or its third-party sub-processors.

As set forth in the MSA, SOW and/or DPAA, a Customer who performs an audit in accordance with this Section must promptly inform OSF on any non-compliance discovered during the audit.

10. PROCESSING OF SENSITIVE PERSONAL DATA

OSF will:

- only process Sensitive Personal Data under the instructions of the Controller

- avoid collection of Sensitive Personal Data where it is not required for the purposes for which the data is collected or subsequently processed
- limit access to Sensitive Personal Data to appropriate persons (by either covering or making anonymous or pseudonymous the data) in accordance with the security standards established in OSF, data protection policies and/or procedures and according to the Controller's instructions
- process Sensitive Personal Data only where the Controller has obtained the individual's *explicit consent* unless the Controller has a legitimate basis for doing so consistent with the requirements of applicable data protection laws.

The responsibility to obtain the consent of the individuals in order to process their Sensitive Personal Data is on the Controller.

Upon Customer's request, OSF shall provide Customer with reasonable assistance needed to fulfil Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent such information is available to OSF.

11. DATA TRANSFER

i. Personal Data transferred by OSF to an OSF Entity as Sub-Processor located within the EU/EEA

Where OSF transfers on behalf of the Controller Personal Data to an OSF Entity located within the EU/EEA, it shall ensure that the Sub-Processor commits to respect the same obligations as the ones which are binding OSF as Processor.

ii. Personal Data transferred by OSF to an OSF Entity as Sub-Processor located outside the EU/EEA

Where OSF transfers on behalf of a Controller Personal Data to another OSF Entity located outside the EU/EEA, such data transfer is covered by these BCRs.

OSF ensures full transparency regarding the use of these BCRs for the transfer of Personal Data outside the EU/EEA.

OSF Entity acting as Processor should also enter into a written agreement (referred to in Section 7 of these BCRs) with the OSF Entity, acting as Sub-Processor, unless the OSF Entity acting as Sub-Processor is party to the MSA/SOW/DPAA between the OSF Entity acting as Processor and the Controller.

iii. Personal Data transferred by OSF acting as Processor to a third-party Sub-Processor

Where an OSF Entity acting as Processor subcontracts its obligations under the MSA/SOW/DPAA, with the authorization of the Controller, it shall do so only by way of a contract or other legal act under the Applicable Data Protection Law with the External Sub-Processor which:

- specifies that adequate protection is provided as set out in Articles 28, 29, 32of the GDPR, and

- ensures that the same data protection obligations as set out in the MSA/SOW/DPAA concluded between the Controller and Processor and Sections 4, 5, 6, 7, 8.2, 8.3, 11, 12, 13 and 16 of these BCRs are imposed on the External Sub-Processor, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing of Personal Data will meet the requirements of the GDPR.

Additionally to the above, the OSF Entity acting as Processor will only transfer Personal Data outside the EU/EEA to an External Sub-Processor if adequate protection of Personal data is ensured, as provided for under Chapter V of the GDPR such as by signing up to appropriate EU Standard Contractual Clauses adopted by the European Commission or by way of a derogation such as obtaining the explicit consent of Data Subject or as otherwise permitted by the GDPR.

OSF Entity, as Processor, will only transfer Personal Data outside the EU/EEA to an External Sub-Processor in accordance with the instructions of the Controller as set out in the MSA/SOW/DPAA concluded by the OSF Entity with the respective Controller.

12. DATA PROTECTION BY DESIGN AND BY DEFAULT

Considering the provisions of Article 25 and Article 47(2)(d) of the GDPR, OSF will collaborate with the Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the OSF BCR in practice, such as data protection by design and by default.

OSF implements appropriate technical and organizational measures, which are designed to implement data protection principles, such as data minimization, in an effective manner, to facilitate compliance with these BCRs, and to integrate the necessary safeguards into the processing and to protect the rights of Data Subjects, taking into account the nature of the processing and the information available to it.

OSF implements appropriate technical and organizational measures for ensuring that, by default, only Personal Data which is necessary for each specific purpose of the processing are processed, in relation to the amount of Personal Data collected, the extent of their processing, the period of their storage and their accessibility.

Also, OSF implements technical and organizational measures as controller/processor in order to secure that Personal Data processing in its entire lifecycle (collection, processing, use, sharing and destruction). In this regard, OSF implements mechanisms to ensure that Personal Data is only processed when necessary for each specific purpose, starting with the project's requirements analysis phase and throughout the entire project development lifecycle.

For this very purpose, where a project is developed, the responsible team in charge of a new processing shall fill in the Registry regarding the data processing operations (the "Registry") all the relevant information related to all categories of processing activities carried out on behalf of Controller. The model of the Registry constitutes Annex 9 of the OSF BCR.

When necessary, as per GDPR requirements and relevant EU/EEA member state data protection legislation, the processing of Personal Data with the potential for a significant privacy impact will be subject to detailed review and evaluation - privacy impact assessment (PIA).

13. NEW BUSINESS OPPORTUNITIES

Where OSF intends to develop new businesses opportunities or to merge with or acquire a company, OSF shall consider all the relevant data protection aspects.

In such cases, the Data Protection Officer (DPO) designated by OSF shall be involved from the beginning of the project until the end. The Data Protection Officer shall conduct a risk assessment in order to make recommendations and make sure that all data protection aspects are considered, enabling OSF to ensure that the new OSF Entity is effectively bound by the OSF BCR and can deliver compliance.

14. OSF COMPLIANCE DEPARTMENT

In order to secure the fact that OSF Processor BCRs are effectively implemented by all OSF Entities, a dedicated compliance department is created. This department is composed of three branches which shall cooperate and work together:

- the legal branch
- the IT and security branch, quality management, and
- the data protection branch

The organization chart for the Compliance department as well as the relevant functions are described in OSF Organizational Chart Diagram (Annex 1).

15. KEY PERFORMANCE INDICATORS

In order to ensure an effective implementation of these BCRs, OSF compliance department maintains key performance indicators (KPIs) as designed by the Data Protection Officer.

These KPIs cover in particular, but not exclusively:

- number of complaints from employees.
- number of requests for access to Personal Data.

- number of data loss cases.
- number of notifications to Supervisory Authorities.
- number of EU standard contractual clauses signed to frame international data transfers.

Data Protection Officer collects these KPIs which are then centralized and analyzed by OSF compliance department every six (6) months.

16. INVESTIGATION

When an on-site investigation takes place, the Data Protection Officer shall be immediately informed.
As described in these BCRs, the Data Protection Officer shall actively cooperate with the Supervisory Authority carrying on the investigation.

17. UPDATES OF OSF BCR

OSF may update the OSF BCR with prior consultation of other relevant stakeholders within OSF such as the Data Protection Officer, Chief Executive Officer, Chief Operation Officer and Legal department. All changes to the OSF BCR shall be communicated to OSF Entities bound by the OSF BCR, to the relevant Supervisory Authorities, via the competent Supervisory Authority and to the Controller.

OSF Legal Department shall be responsible for keeping a fully updated list of OSF Entities and third-party sub-processors involved in the data processing activities for the Controller which shall be made accessible to the Controllers, Data Subjects and Supervisory Authorities, via the competent Supervisory Authorities. Also, OSF Legal Department will keep track of and record any updates to the rules and provide the necessary information systematically to the Controller and to Supervisory Authorities upon request.

OSF shall not transfer Personal Data to a new OSF Entity until such BCR member is effectively bound by the OSF BCR and can deliver compliance.

Any changes to the OSF BCR and/or the list of OSF Entities shall be reported once per year to the relevant Supervisory Authorities, via the competent Supervisory Authority, with a brief explanation of the reasons justifying the update.

Where a change of these BCRs would affect the level of protection provided by the OSF Processor BCRs or significantly affect these BCRs (i.e. changes in the bindingness), it shall be promptly communicated to the relevant Supervisory Authorities via the competent Supervisory Authority, as well as to the Controller.

Where a change affects the processing conditions, the information should be given to the Controller in such a timely fashion that the respective Controller has the possibility to object to the change or to terminate the contract before the modification is made

(e.g., on any intended changes concerning the addition or replacement of subcontractors, before the data are communicated to the new sub-processor).

18. ANNEXES

The Annexes mentioned below are part of the OSF Processor BCRs:

1. Annex 1 – Organization of the Data Protection Community and Roles
2. Annex 1.1. – Job Description – Data Protection Officer
3. Annex 1.2. – Job Description – Security Manager
4. Annex 1.3. – Job Description – System Security Engineer
5. Annex 2 – List of OSF Entities bound by the OSF Processor BCRs
6. Annex 3 - Services to which OSF BCR applies
7. Annex 4 - Matrix of internal roles and responsibilities
8. Annex 5 – Data Subject Access Request Procedure
9. Annex 6 – Complaint Handling Procedure
10. Annex 7 – Technical and organizational measures
11. Annex 8 – OSF BCR Compliance Audit
12. Annex 9 – Registry of data processing operations

MODIFICATION/REVISION REGISTRATION FOR: "OSF Processor BCRs",

DOCUMENT CODE: BCR-OSF-01

	Performed modification				Modification operator		
#	No. §	Page	Date	Modification generating document	Name	Sign.	Date
1							
2							
3							
4							
5							
6							
7							
8							
9							