Calea Plevnei nr. 159, Cladirea C,
Etajul 4, Sector 6, Bucuresti, Romania
Fax: +40 (31) 710 72 91
osf.digital

OSF BCR Compliance Audit

This Annex describes the formal assessment process adopted by OSF to ensure compliance with as required by the Supervisory Authority, and it is a way in which OSF ensures that the provisions of the OSF Processor BCRs are observed and corrective actions are taken as required.

OSF shall maintain an audit program to help ensure compliance with the OSF Processor BCRs, internal verification and audits by Customers.

The compliance audit will assess all the aspects documented in the OSF Processor BCRs and OSF GDPR available documentation, by auditing all relevant OSF's IT systems, data bases, project related environments and documentation, as well as the physical security/access control systems of OSF.

1. Audit plan & programs planification.

OSF's Data Protection Officer/DPO together with the OSF's Top Management decide on the recurrence of performed audits, audit plan and related programs, as well on the scope of the compliance assessment. The following types of internal audit may be performed:

1. At Tool/Application level
2. At project level based on the security & compliance surveys
3. At support department level

The entire internal audit process will be carried out based on OSF Internal Audit procedure, code PS-OSF-04.

Also, in the event that a Customer exercises its right to assess OSF for compliance with the OSF Processor BCRs, such assessment may be undertaken by that Customer, or by independent and suitable auditors (third-party auditor that is not a competitor of OSF) selected by that Customer, as required. OSF's Customers (or auditors acting on their behalf) may assess compliance with the commitments made in the OSF Processor BCRs, in accordance with the terms of the relevant Customer's contract concluded with an OSF Entity. The assessment of compliance may consist of:

- the provision by OSF of written information that may include data related to its sub-processors, or
- interviews with OSF's IT personnel. OSF will not provide a Customer with access to any part of IT systems or infrastructure which process Personal Data of other Customers.

2. Responsible entities - OSF internal audit team.

The OSF BCR compliance audit will be conducted by the OSF's QMS department (Internal audit team), with a close collaboration with the OSF's operations department, IT Infrastructure team, Projects representatives, Support departments representatives, Compliance Team and DPO.

The OSF internal audit team is composed by one Chief Auditor and two Internal Auditors.

3. Time & recurrence of audit

The compliance audit shall be carried out on a regular basis (e.g. annually), with no more than 3 years between each audit. Also, the audit may also occur by demand, requested by the OSF's Top Management and/or other entitled entities/authorities.

4. Coverage of the internal audit:

A. At tool application level, audits will be performed for the following:
   - JIRA
   - ZOHO
   - Confluence
   - Community
   - Service Management
   - GitHub
   - TestLink
   - DocuSign
   - Office 365 environment (Mail, SharePoint, OneDrive, PowerBi, Power Automator, MS project, etc.)
   - Slack
   - Marketo
   - NetSuite
   - SalesForce

B. At project level, a number of X projects will be selected and audited. All Delivery Centers/Business Units must be covered.

C. At support department level, one person will be audited from each support department that handles Personal Data. The support departments that may be subjected to internal audit are: Administrative, Financial, Human Resources, Legal, Quality Management, Operations, Recruiting, Sales, Marketing, and IT Infrastructure.

The review of the contractual terms (related to OSF BCR) is performed by the legal department of OSF, together with the Security Director and aVP of IT Infrastructure.

5. Result of the audit. Corrective and preventive actions

The Lead auditor is responsible for the communication of audit results to OSF's Data Protection Officer, as well to OSF's Compliance team (including Top Management) and corrective actions shall be proposed, if the case.

Corrective and preventive actions will be provided by OSF's auditors together with the aVP of IT Infrastructure & Security Director in accordance with found nonconformities and will be implemented at department/project level by process owners (department manager, project manager).

OSF's DPO must ensure that any actions identified to implement the OSF BCR take place and bring to the attention of OSF's Top Management any report indicating unsatisfactory compliance (in relation to the OSF BCR).

Upon request and subject to applicable law and respect for the confidentiality of the information provided, OSF will:

- provide copies of the result of the audit/ of any assessment of compliance with the OSF Processor BCRs to the relevant Supervisory Authority
- provide a copy of the result of the audit to the Customer, to the extent that the respective assessment relates to personal data OSF processes on behalf of that Customer

<YYYY> Internal Audit Plan

Audit Code	Month	Month	Month	Month
Tools / Software Development DC, BU / Support department	All audited tools (JIRA, ZOHO, Confluence, Service Management, GitHub, Office 365 Environment, Slack, Marketo, SalesForce)	All delivery centers (projects with PII processing to be selected from each delivery center)	Administrative Financial Sales Marketing Legal	Recruiting HR Management Infrastructure Operations
Audit Code	ASC-App-1	ASC-Dev-14	ASC-Sup-04	ASC-Sup-05
Chief Auditor	DPO	DPO	DPO	DPO
Actual date	MMM-YY	MMM-YY	MMM-YY	MMM-YY
Initiating CA/PA	DD-MMM-YY	DD-MMM-YY	DD-MMM-YY	DD-MMM-YY
Implementing CA/PA	MMM-YY	MMM-YY	MMM-YY	MMM-YY

MODIFICATION/REVISION REGISTRATION FOR: "OSF BCR Compliance Audit", DOCUMENT CODE: BCR-OSF-01_A8

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