Contents

Checklist Technical and Organisational Measures (TOM)

1. Introduction

1.1. Terms and definitions

- *Company*: the legal entity with which Constellium signed a contract that requires access to Constellium personal data.
- *Employee*: the employee or employees that the Company employs and that are designated to work on behalf of Constellium in order to fulfill the contract.
- *Computer*: The laptop, PC or any other kind of computing device used by the Employee to access the Constellium IT environment in order to fulfill the contract.
- *Personal Data Protection:* the followings terms shall have the meaning defined in the Regulation (EU) 2016/79 of 27 April 2016 (General Data Protection Regulation, "GDPR"):
    - Controller;
    - Data Subject;
    - Personal Data;
    - Processing;
    - Processor.

1.2. Applicability

This checklist can only be used in different scenarios which can be described as follows:

<u>Scenario 1:</u>

- The Company supports Constellium in development or operation of the Constellium internal IT environment.
- Access is performed remotely (through network connection) or locally through equipment owned and operated by the Company.
- No personal data leaves the Constellium IT environment.

In this case, the relevant chapters are: 2.1 Client security, 2.3. Logical access, 2.4. Logical security, 2.5. Security- and Privacy awareness, 2.8. Contracting/Subcontracting.
Examples: Application maintenance services (AMS)

Scenario 2:

- The Company provides services on applications and servers and is hosting servers or applications in their premises which are located within EU and countries with adequate level of protection according to a decision of the European Commission (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).
  In this case, all chapters need to be considered in the response except 2.6.Transfer.
  Examples: Hosting contracts including maintenance services on different levels (OS, DB, Application)

Scenario 3:

- Same as Scenario 2, but the personal data are potentially transferred out of EU and not to a country with adequate level of protection. In this case, all chapters need to be considered in the response.

  Examples: Hosting outside EU. AMS services provided completely or partly from outside EU.

Scenario 4:

- Applications and servers are hosted within Constellium, services are also provided internally by Constellium.

  In this case, all chapters need to be considered in the response.

  Example: Internally hosted and maintained payroll systems

1.3. How to …

- The Checklist set out the complete requirements of Constellium for the data privacy compliance. There are different scenarios for the services provided. Depending on the scenario, there is only a subset of the questionnaire to be filled out (see 1.2)

Checklist Technical and Organisational Measures (TOM)

- Check the appropriate box to indicate the level of compliance with the requirements:
    - If you fully comply, check (“Yes”) and then use the (“How?”) Column to provide more detailed descriptions of how the security measures have been implemented and provide references to documents like security polices etc.
    - If you do not comply at all check (“No”), and justify why this control is not available.
    - If you are partially compliant, check (“Partly”) then describe the deviation to full compliance.

- Leaving the last column empty is not accepted.

Supplementing this checklist with references to existing Company IT Security documents is required. PDF-Versions of such documents must be provided.

Once you filled out the checklist, please return it to Constellium with all supporting relevant documents. From this checklist and documents, Constellium will elaborate an appendix named “*Technical and organizational measures*” to which the data privacy clause of the contract will refer in order to comply with the GDPR, especially articles 28 and 32 of the GDPR.

2. Checklist

2.1. Physical Security – Clients

Physical security (from where access is performed) must be provided by the Company so the Computer used to access the Constellium IT system is secured from non-authorized physical access.

Nr.	Name	Description	Compliance"	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.1.1	Attended Entry	The office where the Computer is located is only accessible through an attended entrance.	☐ Yes ☐ No ☐ Partly	

2.1.2	Access Control to Office	Everyone entering the office must be identified and authorized before entering.	☐ Yes ☐ No ☐ Partly	
2.1.3	Video Surveillance of Entry Points or Office Space	All entry points to the office have a video surveillance system which is actively monitored.	☐ Yes ☐ No ☐ Partly	
2.1.4	Full Disk Encryption	In case the Computer may leave the office (i.e. the physically secure environment) then it must have full disk encryption applied.	☐ Yes ☐ No ☐ Partly	

2.1.5	Theft Protection	In the office the Computer is secured in order to prevent theft or to make theft more difficult.	☐ Yes ☐ No ☐ Partly	
2.1.6	Walkarounds	Out of office hours the office space is secured by irregular walkarounds of guards.	☐ Yes ☐ No ☐ Partly	
2.1.7	Badges for Guests and Externals	Non-Employees (i.e. Guests) are identified with visible Badges.	☐ Yes ☐ No ☐ Partly	
2.1.8	Others	Please explain other measures you have in place		

2.2. Physical access control – data processing facilities

Nr.	Name	Description	Compliance”	**How?** In case of “Yes” **Justification** in case of “No” **Description of deviation** in case of “Partly”
2.2.1	Attended Entry	The office where the data processing facilities are located is only accessible through an attended entrance.	☐ Yes ☐ No ☐ Partly	
2.2.2	Access Control to the data processing facilities/server rooms	Everyone entering the data processing facilities must be identified and authorized before entering. The access must be documented.	☐ Yes ☐ No ☐ Partly	

2.2.3	Video Surveillance of Entry Points or data processing area	The data center area is equipped with a video surveillance system which is actively monitored.	☐ Yes ☐ No ☐ Partly	
2.2.4	Access by external parties/guests/cleaning personal/visitors	Access is only possible when authorized, documented and accompanied by company staff.	☐ Yes ☐ No ☐ Partly	
2.2.5	Withdrawal of building access, authorisations and access rights	There are regulations in place to timely remove access to buildings, systems, server rooms in case of termination of employees or 3rd parties.	☐ Yes ☐ No ☐ Partly	
2.2.6	Other	Please explain other measures you have in place		

2.3. Logical Access

Logical access control must be provided to the Company's IT environment used to manage the Constellium IT environment in order to assure only identified and authorized individuals are able to access the Computer.
Preventive and detective measures allow timely identification of and response to unauthorized access attempts.

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.3.1	Authentication of individuals	Every access to an IT System is identified and successfully authenticated.	☐ Yes ☐ No ☐ Partly	
2.3.2	Strong passwords	Password quality is technically enforced and includes at least 8 characters password length, upper and lower case characters and numbers. Passwords used interactively by individuals must be changed at least every 90 days.	☐ Yes ☐ No ☐ Partly	
2.3.3.	Bruteforce Prevention	A mechanism is put in place that successfully prevents password brute-force attempts.	☐ Yes ☐ No ☐ Partly	
2.3.4	Vulnerability management	Penetration tests and vulnerability tests are carried out on a regular basis	☐ Yes ☐ No ☐ Partly	

2.3.5	Strong Authentication	Access to highly-sensitive systems areas and remote access to the IT systems are authenticated with a strong authentication technique (two factor authentication).	☐ Yes ☐ No ☐ Partly	
2.3.6	Identity Management	Appropriate identity management is in place that assures new identities for getting access are properly approved and non-used identities are deleted in a timely manner.	☐ Yes ☐ No ☐ Partly	
2.3.7	Traceability	All events surrounding the authentication process, approving creating and deleting of accounts are logged to provide traceability.	☐ Yes ☐ No ☐ Partly	
2.3.8	Authorisation concept	There is an authorisation concept in place to grant company employees access to Constellium's data and systems. Granting authorisations, periodical reviews and revoking authorisations is documented and follows the need to know principle.	☐ Yes ☐ No ☐ Partly	
2.3.9	Logging	Any Modification of Personal Data is logged. Access to log files is restricted.	☐ Yes ☐ No ☐ Partly	
2.3.10	Other	Please explain other measures you have in place		

2.4. Logical Security

The Computer and the IT environment of the Company provide good security so that accessing the Constellium IT environment and processing Constellium's personal data is done in a safe and secure way.

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.4.1	Auditing of Security Events	Security relevant events like authentication events, account modification events, privilege escalation events, blocking and accepting of network traffic in case a firewall is available etc. are written to a protected logfile.	☐ Yes ☐ No ☐ Partly	
2.4.2	Screen Lock	After 15 minutes (or less) of inactivity, all screens are locked and required username password authentication to unlock.	☐ Yes ☐ No ☐ Partly	
2.4.3	Reducing Attacksurface	All IT systems are configured so that the attack surface is reduced to a minimum. This includes: - Deactivation of non-needed device interfaces - Disabling of non-needed services - Deinstallation of non-needed software	☐ Yes ☐ No ☐ Partly	

2.4.4	Regular Software Updates	Whenever security relevant updates are available, they are applied at minimum within 30 days.	☐ Yes ☐ No ☐ Partly	
2.4.5	Malware Protection	Every Server, Laptop and PC has an up to date and effectively configured malware protection systems that allows central reporting and monitoring.	☐ Yes ☐ No ☐ Partly	
2.4.6	Desktop Firewall	IT systems that leave internal networks (i.e. Laptops) have a desktop firewall that prevents incoming network connections when the device is in untrusted networks.	☐ Yes ☐ No ☐ Partly	
2.4.7	Use of Proper Software	Any software that is installed on any IT system is centrally verified and approved by IT and/or IT Security.	☐ Yes ☐ No ☐ Partly	
2.4.8	Network Firewalls	The network and especially the interface to the Internet is protected with a restrictive firewall that applies the white-list approach and that does not allow access from the Internet directly into the internal network.	☐ Yes ☐ No ☐ Partly	

2.4.9	Intrusion Detection Systems	The network and especially the interfaces towards the Internet is protected by an up-to-date intrusion detection system where each alert is properly evaluated.	☐ Yes ☐ No ☐ Partly	
2.4.10	Log and Event Monitoring	Security relevant events (i.e. series of failed login attempts, identified intrusion attempt, etc.) are monitored and appropriate response is triggered in an automated manner.	☐ Yes ☐ No ☐ Partly	
2.4.11	IT Security Policy	The Company has a written - IT Security policy - a data privacy policy - a confidentiality policy and a - Code of Conduct in place that is approved by Company's top management.	☐ Yes ☐ No ☐ Partly	
2.4.12	IT Security Audits	The Company carries out internal and/or external audit of its security measures on an annual basis.	☐ Yes ☐ No ☐ Partly	
2.4.13	Other	Please explain other measures you have in place		

2.5. Security and Privacy awareness

The Company assures that the affected Employees are well aware of proper and secure behavior and of the European privacy laws and its implications.

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.5.1	Security Awareness Training	Employees working for Constellium receive at least yearly basic IT security awareness training which includes: - Introduction to the dangers and threats in the Internet - Detailed information on safe and secure behavior in the Internet - Detailed information on safe usage of e-mail - Detailed information on how to securely transfer data over the Internet - Detailed information on malware infection - Detailed information on phishing attacks - Detailed information on social engineering	☐ Yes ☐ No ☐ Partly	

2.5.2	Privacy Awareness	Employees working for Constellium receive at least yearly basic privacy awareness training	☐ Yes ☐ No ☐ Partly	
2.5.3	Confidentiality Agreement	The Company request their Employees and subcontractors to sign a confidentiality agreement for Personal Data as required by GDPR, which forbids Employees to copy, extract and transfer Constellium's Personal Data (or customer data in general) other than requested by Constellium.	☐ Yes ☐ No ☐ Partly	
2.5.4	Other	Please explain other measures you have in place		

2.6. Transfer

The Company must apply organizational measures to prevent transfers of Constellium's personal data outside EU.

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.6.1	Prevention of Data Transfer	The Company implements organizational measures to ensure personal data is not transferred out of Constellium without prior agreement.	☐ Yes ☐ No ☐ Partly	
2.6.2.	Documentation of approved data transfer	Approved data transfer is documented and a logfile is maintained.	☐ Yes ☐ No ☐ Partly	
2.6.3	Other	Please explain other measures you have in place		

2.7. Testing, assessment and evaluation

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.7.1	Certifications	Does Company maintain a Security Certification (ISO27xxx, others)	☐ Yes ☐ No ☐ Partly	
2.7.2	Incident response process	Feedback procedures are in place to inform the Data Controller on suspected or assumed data loss within 72hours.	☐ Yes ☐ No ☐ Partly	
2.7.3	Other	Please explain other measures you have in place		

2.8. Contracting / Subcontracting

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.8.1	Contractual arrangement	There are clear contractual arrangements with 3rd party service provider and contractors in place. Order management is formalized.	☐ Yes ☐ No ☐ Partly	
2.8.2	Selection of service provider	3rd party service provider and contractors are pre-evaluated and there is a regular supervisory follow-up in place.	☐ Yes ☐ No ☐ Partly	

2.8.3.	Sub-contractor access to privacy data	Sub-contractors, who get access to Constelliums data, comply with the technical and organisational measures agreed in this checklist and have contractually warranted their compliance.	☐ Yes ☐ No ☐ Partly	
2.8.4	Other	Please explain other measures you have in place		

2.9. Availability

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.9.1	Backup	Backups are carried out on a regular basis, the results are monitored daily	☐ Yes ☐ No ☐ Partly	
2.9.2	Backup media	Backup medias are encrypted and stored in a secure distance and place from the data processing facilities.	☐ Yes ☐ No ☐ Partly	
2.9.3	Maintenance	Agreements for the maintenance of IT systems are in place	☐ Yes ☐ No ☐ Partly	
2.9.4	Business Continuity	A business continuity concept is in place, the time to restart after complete destruction of the data center facilities matches with the SLAs defined in the service contract.	☐ Yes ☐ No ☐ Partly	

2.9.4	Other	Please explain other measures you have in place		

2.10. Segregation

Isolated Processing of data which are collected for different purposes or customers

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.10.1	Separation of data is supported by authorisation concept	There is an authorisation concept available which excludes access to data for employees which do not work with / for the Data Controller	☐ Yes ☐ No ☐ Partly	
2.10.2	Data separation	The data are held available in independent data areas per application	☐ Yes ☐ No ☐ Partly	
2.10.3	Network separation	Within the Company network there is a separation on network level for the different clients	☒ Yes ☐ No ☐ Partly	
2.10.4	Segregation on Employee level	Employees are bound in writing not to bring information from the data inventories into other projects/clients	☒ Yes ☐ No ☐ Partly	
2.10.5	Other	Please explain other measures you have in place		

2.11. Pseudonymisation

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.11.1	Pseudonymisation	Pseudonymisation of personal data is implemented In such a way, that data cannot be associated with specific Data Subjects without assistance of additional information which is stored separately and is subject to appropriate technical and organisational measures	☐ Yes ☐ No ☐ Partly	
2.11.2.	Other	Please explain other measures you have in place		

2.12. Anonymisation

Nr.	Name	Description	Compliance	**How?** In case of "Yes" **Justification** in case of "No" **Description of deviation** in case of "Partly"
2.11.1	Anonymisation	personal data are anonymised in such a way, that data cannot re-constructed by any means	☐ Yes ☐ No ☐ Partly	
2.11.2	Other	Please explain other measures you have in place		