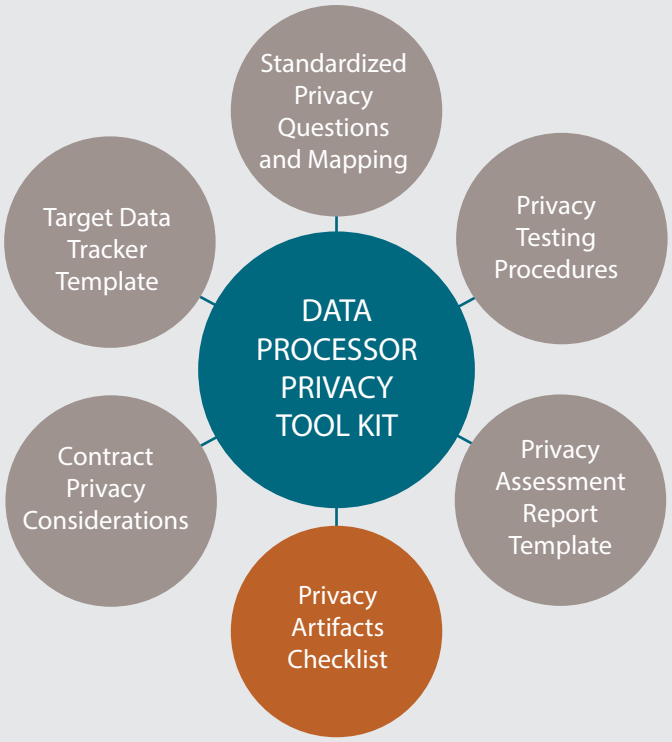
SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING GDPR BEST PRACTICES

GDPR: Data Processor Privacy Tool Kit – Appendix:
Privacy Artifacts in Support of Article 28 – Processor



SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR: Privacy Tool Kit – Appendix
Privacy Artifacts in Support of Article 28 – Processor

GDPR Article 28 specifically addresses and outlines a number of requirements related to data processors. The table in this Appendix addresses the relevant privacy requirements in Article 28 and suggests certain documents, artifacts and evidence in support of conformity with these requirements.

The table below focuses on the two relationships; first being between data controllers and their data processors; and the second being between the data processors and their sub-processors. This Tool Kit component addresses only the privacy-related elements of these relationships.

Additionally, throughout the GDPR there are many security related requirements in regard to controllers, processors, and sub-processors. This table does not address the security requirements, as this Artifacts component of this Tool Kit is limited to privacy concerns. *Note: for Assessment Tools that are mapped to security, breach notification and other GDPR components outside of privacy, please visit www.sharedassessments.org.*

Using this table as part of initial due diligence or on-going monitoring, a controller might request from a processor some or all of the identified documents, artifacts and evidence. Likewise, a proactive processor might use this table to develop and prepare a package for its controllers that contains some or all of the identified documents, artifacts, and evidence and specifies the steps they have taken to conform with the privacy related items in Article 28.

Please note that the Working Party (i.e., the group of 28 countries), the EU Commission, and member states are still refining their guidance and enacting local regulations in regard to parts of the GDPR. We therefore anticipate that this table will be updated over time, as these parties further identify and refine their privacy requirements.

Link to the full General Data Protection Regulation can be found at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

APPENDIX: GDPR ARTICLE 28 PRIVACY ASSURANCE ARTIFACTS CHECKLIST

GDPR ARTICLE.PARAGRAPH	GDPR CLAUSES	POTENTIAL RECOMMENDED ARTIFACTS
28.1	"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."	• Controller/processor Contracts • Privacy tab of Standardized Information Gathering (SIG) questionnaire • Privacy section of Standardized Control Assessment (SCA) procedures, Service Organization Control (SOC) 2, or other similar attestation • Other processor supplied evidence such as policies and procedures, and assurance or certification of relevant privacy related technical and organizational measures
28.2	"The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors."	• List of sub-processors including specific written authorization • In the case of general authorization, the section of the contract containing the general authorization • Documentation provided by the processor that the controller has acknowledged via email, post mail, or other notifications; updated contract addendum, or any other means and has approved the use of each sub-processor • Evidence of processor's Vendor Risk Management Program for their sub-processors including policies and procedures, risk ratings, due diligence policies, procedures, and tools, certifications, attestations, and third party reviews such as the SCA or SOC 2
28.3	"Processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."	• Templates and fully executed Master Services Agreements (MSA), including privacy clauses and addendum • Fully executed Statements of Work (SOW) • Documentation of data elements to be used by the processor via the SOW or other document (e.g., customer names, addresses, other privacy-related data)
28.3.a	"Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest."	• Evidence, certification, attestation of processing of personal data only on instruction from controller in contract or Statement of Work. Such evidence, certification, attestation potentially to include privacy tab of SIG, privacy section of SCA, SOC 2, or other similar attestation • List of valid transfer method for each non-EU sub-processor, such as model contracts/clauses, binding corporate rules, Privacy Shield, adequate country designation

APPENDIX: GDPR ARTICLE 28 PRIVACY ASSURANCE ARTIFACTS CHECKLIST		
GDPR ARTICLE.PARAGRAPH	**GDPR CLAUSES**	**POTENTIAL RECOMMENDED ARTIFACTS**
28.3.b	"Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality."	• Privacy Policy • Confidentiality and/or Non-Disclosure Agreements (NDA) • Code of Ethics containing relevant privacy sections, and individual certifications • Clauses in employee contracts and the like • Any additional confidentiality statements • Evidence of the existence of onboarding and at least annual privacy and security programs and training along with test completion data for each individual
28.3.e	"Taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, in so far as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's right laid down in Chapter III."	• Evidence, certification, attestation including policies and procedures, privacy tab of SIG, privacy section of SCA, SOC 2, or other similar attestation in regard to personal data supplied by the controller and related to: o Section 1 – Transparency and modalities o Section 2 - Information and access to personal data o Section 3 - Rectification and erasure o Section 4 – Right to object and automated individual decision-making o Section 5 – Restrictions
28.3.g	"At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data."	• Letter from the processor as to the destruction of data • Certificates of destruction (e.g., National Association for Information Destruction - NAID) • Processor data retention policies
28.3.h	"Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."	• Due Diligence (SIG, SCA) SOC, ISO exams, etc.) • Audit reports (SOC, internal audits) • Right to audit clause in contract • Policies, Procedures, Standards – including periodic approvals
28.3	"With regard to point (28.3.h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions."	• Communication from Processor to Controller that a request cannot be performed as it may violate GDPR

APPENDIX: GDPR ARTICLE 28 PRIVACY ASSURANCE ARTIFACTS CHECKLIST

GDPR ARTICLE.PARAGRAPH	GDPR CLAUSES	POTENTIAL RECOMMENDED ARTIFACTS
28.4	"Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation."	• Processor's sub-processor contract template and privacy clauses and addendum • Sample of executed sub-contractor contracts and privacy clauses and addendum
28.9	"The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form."	• Sample of executed sub-contractor contracts and privacy clauses and addendum

SFG | SHARED ASSESSMENTS

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted source in third party risk assurance, is a member-driven, industry-standard body with tools and best practices, that injects speed, consistency, efficiency and cost savings into the control assessment process. Shared Assessments Program members work together to build and disseminate best practices, building resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments.

P: (505) 466-6434
F: (505) 466-3111
E: info@santa-fe-group.com