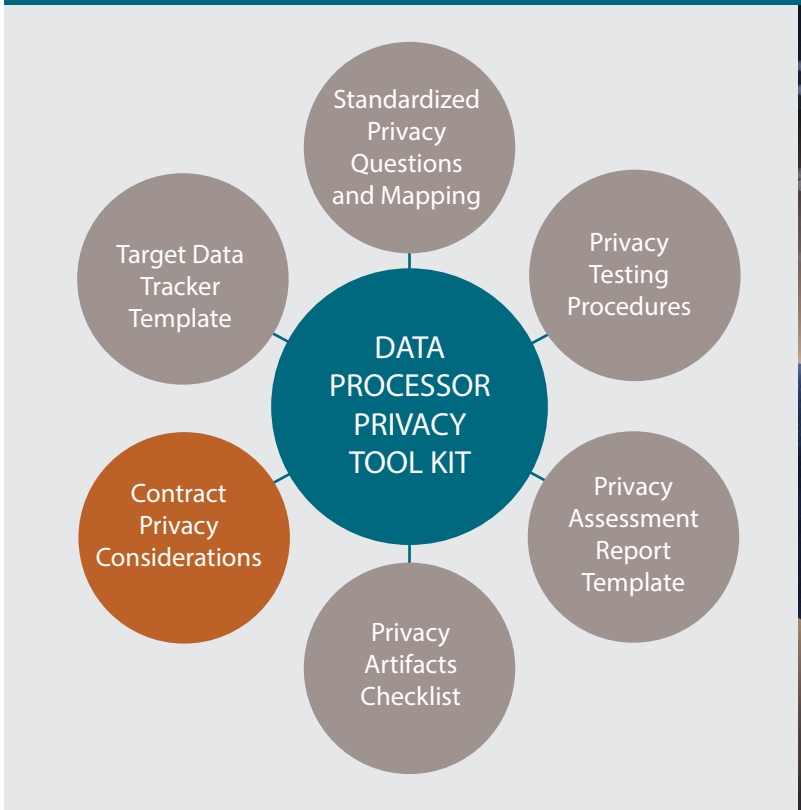
SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING GDPR BEST PRACTICES

GDPR: Data Processor Privacy Tool Kit – Appendix:
Article 28 Contract Privacy Considerations



SFG | SHARED ASSESSMENTS

BUILDING GDPR BEST PRACTICES:

GDPR Privacy Tool Kit – Article 28 Contract Privacy Considerations

Article 28 of the GDPR contains a number of items regarding contracts that are specific to roles involved in data processing.

The contract considerations included in this Appendix focus on two relationships; first: between data controllers and their data processors; and second, between data processers and their sub-processors. This component of the Tool Kit addresses only the privacy-related elements of these relationships. Additionally, throughout the GDPR there are also many security related and other requirements such as breach notification. *Note: for Assessment Tools that are mapped to security, breach notification and other GDPR components outside of privacy, please visit www.sharedassessments.org.*

Incorporating some or all of these requirements in a formal contract or addendum will allow a controller to engage a processor in a manner that is consistent with the GDPR. Likewise, a proactive processor might develop its own contract or addendum that reflects the services and products it supplies to controllers and to those contracted to a sub-processor.

We recommend that controllers and processors share these contract considerations with the legal counsel of their choice, in order for counsel to develop appropriate language for incorporation in contracts and addendum.

Please note that the Working Party (i.e., the current 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 the parties further identify and refine their privacy concerns.

Additional Data Controller Considerations

Any contracts including existing ones that are in place on May 25, 2018, and new ones after this date will be required to conform to the GDPR.

Data controller obligations under GDPR will trigger additional contract provisions based on the scope of work, category of personal data, and the types of data processor relationships. Article 24 (1), Article 29 and Article 46(1) define specific obligations for controllers that impact data processing and thus the data processor contract. Operational considerations for the processing of data and appropriate safeguards will trigger additional data protection contract provisions.

It is essential to a comprehensive review of contract privacy considerations, that a complete inventory of all data controller and data processor contracts be created and maintained.

APPENDIX: ARTICLE 28 CONTRACT PRIVACY CONSIDERATIONS

CONSIDERATIONS	RESPONSIBLE PARTY	DONE	DATE
• A contract is required when a controller uses a processor, and when a processor uses a sub-processor			
• Contracts should set out:			
o The subject matter of the processing			
o The duration of the processing			
o The nature and purpose of the processing			
o The type of personal data and categories of data subject			
• Contracts should also include the following terms requiring the processor to:			
o Only act on the written instructions of the controller			
o Ensure that the data processor is subject to a duty of confidence			
o Only engage sub-processors with the prior consent of the controller and under a written contract			
o Assist the data controller in providing in providing data subjects access and allow them to exercise their rights under the GDPR			
o Delete or return all personal data to the controller as requested at the end of the contract			
o Submit to audits and inspections			
o Provide the controller with the information it needs to ensure that they are both meeting their Article 28 obligations			
o Inform the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state			
• Processor to provide at least annually, subject to controller review and acceptance			
o Completed SIG Privacy Tab or similar assessment			
o Completed third party attestation such as the SCA and/or SOC 2 *			
o Code of Ethics containing Privacy Section			
o Evidence and results of Code of Ethics training and certification by each individual with access to Personal Data			
o Privacy Training Program			
o Evidence and results of Privacy training and certification by each individual with access to Personal Data			
o Written documentation on data repositories, data flows, and processing			
• Terms and conditions of controller to processor contracts should flow down to sub-processors			
• For international transfers of Personal Data from the EU, specify the legitimizing method utilized: e.g., model contracts/clauses, binding corporate rules, Privacy Shield, adequate country designation			

* Such as, Shared Assessments' Standardized Control Assessment (SCA) SCA Privacy Testing Procedures (formerly the Shared Assessments' AUP) and/or Service Organization Control (SOC) 2 or International Standard on Assurance Engagements (ISAE) 3402.

SOURCES

The primary sources for this section include:

1) GDPR Article 28. https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf)

2) ICO GDPR guidance: Contracts and liabilities between controllers and processors. https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

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