The Ultimate Vendor Risk Management Handbook

JANUARY 9, 2019
UPDATED: JANUARY 25, 2019

GUIDE

OneTrust
Privacy Management Software

Table of Contents

Understand Terminology and Requirements

New obligations under the GDPR

The General Data Protection Regulation (Regulation (EU) 2016/679, 'GDPR') has brought along a set of new obligations for both the personal data controllers and processors. Probably most important is the liability shift introduced by the legislation – organizations are now liable for their vendors and must always demonstrate that they put all reasonable consideration into choosing those that comply with the GDPR.

Amongst other requirements, it makes written contract between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures under the Data Protection Agreement). Furthermore, the GDPR's Article 28 outlines a robust set of mandatory minimum terms that must always be present in every data processing agreement. As the GDPR does not grandfather in pre-existing contracts, it requires for all pre-existing controller-processor contracts to have been brought into compliance with its requirements by its effective date: May 25, 2018.

Very important change affecting the overall obligations under the GDPR is the fact that for the first time, the personal data processors have direct statutory obligations for certain data protection matters, and statutory liability (including the possibility to incur regulatory fines) for breach of their respective obligations under the GDPR. In addition, the data processors (along with the data controllers) are also liable for direct damage compensation claims brought forth by data subjects. Such claims can be also pursued through class action lawsuits, as the GDPR envisions – and we can already see first examples of this new practice emerging in relation to recent cases of Cambridge Analytica-Facebook and British Airways breach.[1]

---

1 Facebook and Cambridge Analytica news on class action: https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit
British Airways Breach and Class Action news: https://www.forbes.com/sites/kateoflahertyuk/2018/09/20/how-the-british-airways-breach-will-reveal-the-true-cost-of-gdpr/

Due to the novelty of the GDPR, there remains a significant number of practical unclarities and issues to be addressed in a harmonized way through the enforcement action and perhaps through the guidance and activities of the European Data Protection Board ('EDPB'). For the time being, some EU Member State Data Protection Authorities (including British ICO and Irish Data Protection Commissioner) have been providing guidelines on the new vendor-related obligations and specifics of the relationships.[2]

Controller, processor and joint controllers

In principle, the GDPR retains a similar set of roles as was present under the previous legal regime of the EU Data Protection Directive.

Under the GDPR Art. 4(7), the **controller** is either natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

On the other hand, the **processor** is by GDPR's Art. 4(8) defined quite simply as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

To the two already pre-existent roles, the GDPR adds a new layer by formally acknowledging a relationship of **joint controllers** in its Art. 26(1). It thus labels a situation, where two or more controllers jointly determine the purposes and means of a particular personal data processing.[3]

While the actors and their description did not contain much change under the GDPR, it turns out that in practice, determining who is who in a processing relationship can be very complicated. Particularly the complexity of the online world's marketing platforms creates a lot of uncertainty and it is often left for the Regulatory Bodies and courts to determine the right answer. On that matter, we have seen even the biggest technology companies err in determining their correct data protection roles. In a recent very

---

2 See Consultation: GDPR guidance on contracts and liabilities between controllers and processors, Information Commissioner's Office (consultation period: 13 September 2017 – 10 October 2017) https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/consultation-on-gdpr-guidance-on-contracts-and-liabilities-between-controllers-and-processors/; Guidance: A practical guide to data controller to data processor contracts under GDPR, Data Protection Commissioner http://gdprandyou.ie/wp-content/uploads/2018/05/Guidance-for-Data-Processing-Contracts-GDPR.pdf (providing guidelines on when organizations should enter into a data processing contract under GDPR, and when the minimum provisions which should be included in such a contract).

3 The complete CJEU decision is available here: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130dab47ce2674a0147679d80c811e09ce505.e34KaxiLc3eQc40LaxqMbN4Pb3mRe0?text=&docid=202543&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=117645 CJEU press release on the decision is available here: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081en.pdf

surprising ruling, the Court of Justice of the European Union established joint controller relationship between Facebook and Facebook fan page administrators in relation to the fans' personal data processing.

While there is no one-size-fits-all solution to determining the roles, and it is essential to assess each data processing activity and relationship individually, perhaps the best way to go about it would be to look at who determines the purpose and means of the personal data processing – is that just one party, or are there perhaps several of them (suggesting joint controllership)? On a practical level, the purpose of the processing is typically an answer to the question 'What do we need the personal data for?'. By the same token, the means of processing would answer questions around how the personal data are to be collected, in what extent, for what duration, through which methods will they be processed, what will they be integrated with, how will they be deleted etc.

Responsibility of the controller and processor

As was already annotated, the scope of data protection responsibilities has grown and has become more complex with the GDPR.

It is however still the **controller** who retains the major responsibility to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Such measures will also need reviews and updates where necessary (GDPR Art. 24(1)). The concrete set of measures ensuring compliance with the GDPR are of course individual for each organisation and processing: depending on the nature, scope, context and purposes of the processing. When deciding on the specific organisational and technical safeguards, the controllers should also consider how likely and severe are any risks to the data subjects that may result from the processing. Sometimes, these measures may include implementation of data protection policies by the controller (GDPR Art. 24(2)).

On many occasions, **demonstrating compliance** can be very challenging. For the controllers, this means that every important processing-related decision and process should be somehow documented. This does not necessarily mean paper documentation, but simply any proof (even in the form of training materials or vendor vetting forms) that a process or measure is in place or that it was considered. The GDPR suggests that the adherence to approved GDPR codes of conduct or certification mechanisms can be used as an element for demonstrating the controller's compliance with the GDPR obligations (Art. 24(3)).

This controller's responsibility doesn't vanish even when using vendors for processing of personal data. The controller must always ensure that the processors provide sufficient guarantees to implement appropriate technical and organisational measures for the processing to meet the GDPR's requirements and ensure protection of the data

subjects' rights. This means, that the controller organisation (i) can only use processors with sufficient GDPR compliance guarantees, and (ii) the controller must be able to demonstrate this too. This can be done for example through vendor assessment documentation and vendor audits.

Processor's responsibilities can be even more complex. Primarily, it is key for the processor to maintain adequate technical and organisational measures to ensure GDPR compliance of the processing and protection of the data subject's rights. Of this, the processor must be able to provide sufficient guarantees to the controller for the duration of their relationship (GDPR Art. 28(1)). Again, this can be done through audits, certification, etc. However, at the same time, the processor would very often engage other vendors for help with certain portions of the processing. GDPR however limits processor's leeway by requiring that every new sub-processor can only be engaged with prior specific or general written authorisation of the controller.

In practice, the GDPR requires everyone down the vendor supply chain (from primary processors to sub-processors all the way to their sub-processors) to be constantly aware of who are the vendors processing the specific sets of personal data relevant to the original controller-processor agreement. Furthermore, it requires everyone within the supply chain to (i) comply, (ii) demonstrate compliance, and (iii) ensure their vendors' compliance with relevant obligations of the original controller-processor agreement. Some of these contractual obligations will simply keep shifting in the same scope down the vendor supply chain.

It is also important to remember that any processing of personal data on the side of processors and sub-processors must be generally governed by the data protection agreement. In addition, the GDPR Art. 29 stresses that any person acting on behalf of the controller or processor, who has access to personal data, shall not process those data except on instructions from the controller (or based on mandate by EU or Member State law). In practice, this is a requirement for good clarification of what is included in the required processing activities within the Data Processing Agreement, as anything beyond that could be perceived as processor's breach of the GDPR compliance obligations. Processor (and any sub-processors) can only act within the boundaries of the controller's instructions.

From the perspective of **joint controllers**, it is essential for them to mutually clarify their respective portion of their GDPR obligations and responsibilities towards the data subjects. This mutual arrangement should be made available to the data subjects and should include the split of responsibilities for compliance with each of the controller obligations under the GDPR, their duties to comply with data subject requests and exercise of the data subjects' rights. It is however also good to remember, that the data subject can still exercise his or her GDPR-related rights against either of the joint controllers.

To summarize, the main requirements for all parties involved is not only to ensure GDPR compliance, but also to demonstrate their compliance and compliance of those that are below them in the vendor supply chain. Organizations must take responsibility for not only their own data protection measures, but also for those of their vendors.

Transfers of personal data outside the EU

Besides the material obligations of the vendors, the territorial transfer of personal data between countries must always be considered in the vendor relationships involving personal data.

For the transfers within the EU/EEA area, there are no additional obligations to comply with and it is generally sufficient to have a written data protection agreement between the parties. However, the transfer of personal data outside the EU/EEA zone can only be done if one of three GDPR-outlined transfer conditions is met. These three conditions are: (i) adequacy decisions, (ii) appropriate safeguards, and (iii) derogations. These are to be pursued in order as they are described, i.e. if an adequacy decision is available for the transfer, it should be used preferentially rather than seeking appropriate safeguards or derogations instead.

Adequacy Decisions

In practice, if planning to transfer personal data to vendor organization that is based outside the EU/EEA area, it is best to start by checking whether there is an adequacy decision in place for the relevant territory or even particular sector within such territory. The current list of adequacy decisions in effect can be found at the website of EU Commission, which is also the institution that on behalf of the EU issues adequacy decisions. Adequacy decisions (described in GDPR Art. 45) are issued by the Commission to mark that a certain country, territory or sector awards a level of protection to the personal data and the rights of data subjects, that is adequate to the level of protection in the EU. For that reason, it is good to check regularly for any changes of existing adequacy decisions as these may happen due to Commission's periodic adequacy decisions' review.

On a practical level, an existing adequacy decision means that personal data can flow from the EU (and EEA – Norway, Liechtenstein and Iceland) to a third country without any further safeguards being necessary. In other words, personal data transfers to such country will be perceived similarly to intra-EU transfers. At the time of writing, the Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the U.S. (limited to the Privacy Shield Framework) as providing adequate protection. Adequacy talks are further ongoing with South Korea and a new adoption procedure was launched for adequacy decision on Japan.[4]

The EU – U.S. Privacy Shield Framework is a specific adequacy mechanism because it does not cover all companies established in the U.S., but only those that are self-certified and regularly audited by the U.S. Department of Commerce. If you wish to transfer the personal data to the U.S., you should therefore first check whether the recipient organization has an active privacy Shield certification - only then can you rely on the adequacy decision.

Appropriate Safeguards

If there is no adequacy decision that could cover the transfer of personal data, you can choose to rely on one of the appropriate safeguards outlined in GDPR Art. 46. There are in fact several mechanisms included in the 'appropriate safeguards' group:

i. **Standard contractual clauses** (also known as model clauses) are likely the most frequently used transfer safeguards and they are approved by the European Commission. In practice, an organization looking to transfer data outside the EU/EEA area can use one of the standard contractual clauses as a standard non-negotiable contractual form. The advantage of these clauses is that they don't require regulatory approval and any party looking to use them can simply download the controller-controller or controller-processor version of the clauses and sign them (without changing any provisions) with its respective third country party. The most up-to-date version of the standard contractual clause is always available at the Commission website.

4 European Commission website information as of 05/11/2018, available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

ii. **Binding Corporate Rules** if adopted by an organization in accordance with GDPR Art. 47 can be a particularly good solution for data transfers (including employee data) within global corporations and their groups.

iii. **Approved Codes of Conduct** or **Certification** mechanisms are envisioned by the GDPR as another mechanism facilitating the flow of personal data outside the EU/EEA. Codes of Conduct (outlined in GDPR Art. 40) are best used by associations or other organization representative bodies that come up with EDPB-approved enforceable mechanisms for processing personal data that are binding upon their member organizations across borders. GDPR Art. 42 Certification mechanisms are on the other hand meant to typically ensure GDPR compliance with relation to individual organization's product, service or particular operation.

iv. **Ad hoc contractual clauses** are based on GDPR Art. 46(3)(a) and their advantage is that as opposed to the standard contractual clauses, they can be tailored to the individual situation of the parties. However, they must still conform to the data protection and compliance requirements set out by the GDPR and must also be approved by the relevant Data Protection Authority before any data transfers can begin.

v. **Public International Agreements** allow the organizations to base their personal data transfers on International Treaties and Bilateral Agreements between respective states. There are unfortunately not very many of such agreements, but for example the EU has signed bilateral passenger name record agreements with the U.S., Canada and Australia facilitating transfer of flights passengers' personal data.[5]

Derogations

GDPR in its Art. 49 sets out derogations to be used only in in the absence of adequacy decisions and when none of the Appropriate Safeguards can be applied. In other words, derogations will only be used for a very small spectrum of specific situations where no other transfer mechanisms apply. In such cases, the transfers would be enabled under one of the following conditions: (i) data subject's informed and explicit consent to the transfer, (ii) necessity for the performance of a contract between the data subject and the controller, (iii) necessity for the conclusion or performance of a contract in the interest of

5 More information on the public international agreements can be found on the European Commission website https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en

the data subject between controller and a third party, (iv) necessity for important public interest reasons, (v) necessity for the establishment, exercise or defense of legal claims, (vi) necessity for protection of vital interests of the data subject or other persons where the data subject is incapable of giving consent, (vii) transfer from a register of public information, and (viii) legitimate interests of the controller.

Contractual terms

The GDPR requires for the personal data processing by the processor to be governed either by a contract or other legal act under the EU or Member State law that is binding on the processor. It may be based, in whole or in part, on standard contractual clauses.[6]

The data processing contract (or other legal act) must set out the following:

i. subject matter and duration of the processing,

ii. nature and purpose of the processing,

iii. type of personal data involved in the processing,

iv. categories of data subjects, and

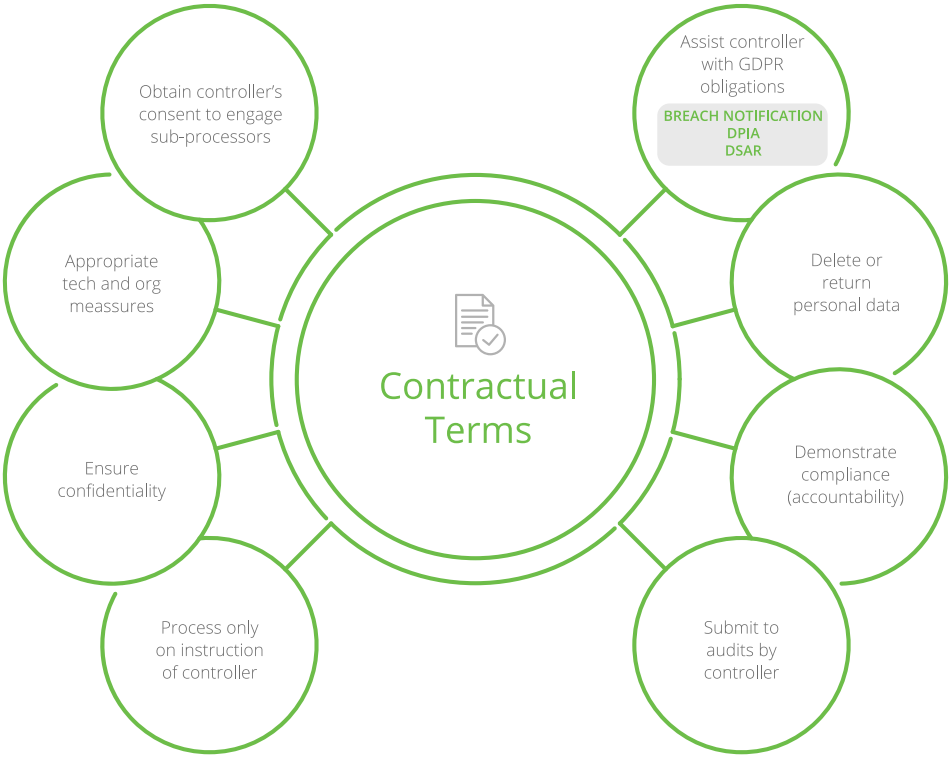
v. obligations and rights of the controller.[7]

---

6 Articles 28 (3), (7) and (8) of the GDPR.

7 Article 28(3) of the GDPR.

In particular, the following **processor obligations** must be specifically stipulated between the parties:



At the same time, the processor is not allowed to engage any sub-processor without prior general or specific written authorization of the controller.

What is then the **difference between general and specific authorisation?**

Under a general authorization, a controller will allow its processor to select, change and terminate sub-processors without getting pre-permission from the controller for each event. However, under GDPR Art. 28(2), the processor still needs to inform the controller of any changes, and to give the controller an opportunity to object to them. On the other hand, the specific authorization requires the processor to seek the controller's approval every time a new sub-processor is to be engaged. See more practical tips in the operational section (Step Seven – Update controller-processor contract).

Furthermore, the same data protection obligations must in relevant portion be imposed on the sub-processor by way of a contract or other legal act. However, the initial processor still remains fully liable to the controller if the sub-processor fails to fulfil its data protection obligations.[8]

8 Art. 28 (4) of the GDPR.

The GDPR does not particularly address the question of **compensation for the additional costs** related to assistance provided by the data processors to the controllers i.e. in relation to audits, DPIAs etc. This is a grey area where arguments are made both ways and probably will depend upon each individual type of relationship to determine the best scope of requirements and appropriate type of compensation arrangement. The controllers can use to their advantage the recently issued guidance by the Bavarian Data Protection Authority, that addresses the practice of some Data Protection Agreements to contain a fee to allow audits by the data controllers. The Data Protection Authority clarified that the exercise of 'controlling rights' over the processor's systems must not be made dependent on any fee or remuneration.[9]

The specific contractual obligations for data processing agreements or legal acts required by the GDPR Art. 28 (3) are part of the graphical overview above and include the following:

i. Processing can only be **based on documented instructions** of the controller (including transfers of personal data outside the EU/EEA). The instructions do not necessarily have to be in writing but must be demonstrable. There is an exception for processing and transfers that the processor must perform based on the EU or Member State law – in such cases, it is enough for the processor to inform the controller of such legal requirements before processing (unless even this is prohibited by the law based on public interest grounds),[10]

ii. **Ensuring confidentiality** of all persons authorized to process personal data.[11]

iii. Appropriate technical and organizational **measures ensuring the security of processing** based on GDPR Art. 32. While the GDPR suggests some particular measures like pseudonymization and encryption, the specific set of measures is left to determine and outline in the contract by the parties based on the specifics of the processing and its particular associated risks,[12]

---

9 Bavarian Data Protection Authority (BayLfD) Guidance AKI 6 available here (in German): https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.html

10 Art. 28 (3) (a) of the GDPR.

11 Art. 28 (3) (b) of the GDPR. It is important to understand this obligation is very wide and even on general, the courts often find that the organisations are liable for malicious actions of their rogue employees. Please see this recent UK Court of Appeal case regarding the company liability for personal data breach caused by its rogue employee: https://privacylawblog.fieldfisher.com/2018/morrisons-loses-its-challenge-over-data-breach-liability-an-important-judgment-for-employers

12 Art. 28(3)(c) and Art. 32 (1) and (2) of the GDPR.

iv. Obtain **controller's authorization to engage or replace sub-processors**, and set out in the sub-processor agreement the same data protection obligations in the contract or other legal act as are contained in the original agreement/legal act with the controller,[13]

v. **Assist the controller** by appropriate technical and organizational **measures for the fulfillment of controller's obligation to respond to data subjects' rights' requests.** However, the nature of the processing and the possibility of such assistance should be taken into account when outlining the scope of this obligation,[14]

vi. **Assist the controller** in ensuring compliance with the GDPR requirements for **security of processing**, personal **data breach notification** to authorities and data subjects, and **data protection impact assessments** ('DPIAs'). Again, the scope of such assistance is dependent on the nature of processing (i.e. whether a DPIA is required) and what information is in fact available to the processor (e.g. if the processor conducts just a marginal portion of the processing, it likely cannot assist with the DPIA by completing all elements of the assessment, as it is simply not aware of them).[15]

vii. At the choice of the controller, **delete or return** all the personal data to the controller (including existing copies) at the end of the processing relationship between the parties.[16]

viii. **Demonstrate its compliance** with all of these obligations through making available the necessary information and allowing for (and contributing to) audits and inspections conducted either by the controller or by a controller-mandated auditor. The provisions of the joint controller agreement should take this into account as well and the controllers should be ready to assist each other in this and many other matters relevant to the processing. As the joint controllership is still not particularly common, it is helpful for the parties to include a more detailed split of responsibilities and operational arrangements into their agreement, because each party's expectations and preconceptions about their role can differ very widely and can cause a lot of compliance and practical issues if not addressed and clarified from the start of the relationship.

---

13 Art. 28(3)(d) and Art. 28(2) and (4) of the GDPR.

14 Art. 28(3)(e) and Chapter III of the GDPR.

15 Art. 28(3)(f) of the GDPR.

16 Art. 28(3)(g) of the GDPR.

Joint Controller Contractual Terms

GDPR does not specifically prescribe a written contract to govern the relationship between/among the joint controllers, but it does envision that some form of arrangement should be in place. It should include the following:

i. Transparent determination of **each party's responsibilities for compliance with the GDPR obligations**.[17] This can be best achieved by listing all the GDPR-mandated controller duties and deciding one-by-one who is responsible for ensuring compliance with them. As the joint controllership is still not particularly common, it is helpful not to underestimate this step because each party's expectations and preconceptions about their roles can widely differ and if left unclarified can cause a lot of compliance issues in the future. For example, clarifying who notifies any personal data breaches to the authorities or perhaps who ensures that processors are correctly audited may go a long way in the day-to-day operations.

ii. Respective **roles and relationships of the controllers towards the data subjects**. It should clearly establish who is responsible for each controller duty relevant to exercising of data subject rights, e.g. who answers individuals' requests for information about data processing. It may be helpful to set up a specific contact point for facilitating these relationships both ways. Essence of this joint controller arrangement should be made available to the data subjects as well. However, the data subjects can still exercise their rights against either of the controllers, so their arrangement should consider this and include mechanism for mutual assistance and passing of information in such cases.[18]

17 Arts. 13 and 14, and Art. 26(1) of the GDPR.

18 Art. 26 (2) and (3) of the GDPR.

Ten Steps to Meet Your Article 28 Obligations

1| Identify whether your organization is a controller or a processor

It is key for each organization to correctly determine its role under the GDPR – this in turn determines all the following steps. While the GDPR does define the controller and processor in its Art. 4(7) and (8) of the GDPR, it is in practice often very difficult to correctly establish who is who in a business relationship (please see the terminology section for more details on each role).

While each processing relationship may be slightly different and has to be approached on a case-by-case basis, there are some practical questions that may help guide you towards the right answer:

i. Who decides what personal information is going to be collected and kept?

ii. Who decides the use to which the information will be put?

On that account, Irish Data Protection Commissioner has produced online guidance and furthermore some older (yet still quite useful) guidance can be found in the Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor".

2| Ensure collaboration between privacy and security professionals

Because GDPR Article 28 requires for controllers to select only such processors that have appropriate technical and organizational security measures in place, where applicable, controllers' privacy teams will need to cooperate with security teams to vet potential processors and to conduct their regular audits. Also, processors' teams will need to collaborate to respond to controller teams' demands and questions.

For these purposes, you should as a start ensure that your Security and Privacy teams are aware of each other's operations and priorities. With the vendor vetting and audits in mind, it would be helpful to combine the teams' efforts in joint vendor assessment form including both privacy and security-related questions – the answers to one group will likely complement the other. Privacy and Security teams should also learn to sync their vendor requirements and can share the burden of vendor management and audits.

3| Get familiar with vendor risk management (VRM)

What is vendor risk management?

Vendor risk management (VRM) is the practice of evaluating business partners, associates, or third-party vendors both before a business relationship is established and during the duration of your business contract. This is an important concept and practice to put in place during the relationship with your vendors and the procurement process. Although VRM is based in information security, it can be very helpful to implement it and embed privacy-related concerns and operations into it as well. Information security and privacy have many overlaps and it makes sense both from the practical and resources' perspective to combine the two.

VRM has three distinctive priorities:

Evaluate	Mitigate	Manage
Assess potential business partners, vendors and associates, before a relationship is established.	Identify potential risks found when evaluating the vendor. Record the resolution response for each risk.	Keep track of all vendor engagements and any associated contracts or documents.

There are several good resources on VRM, but even better may be to align the VRM security and privacy priorities with your existing vendor processes and adjust them to suit both the compliance concerns and your business operations.[19]

Request a live demo of OneTrust Vendor Risk Management.

19 Overview of Vendor Risk Management: https://www.gartner.com/it-glossary/vendor-risk-management . Practical use of VRM with technology: https://www2.deloitte.com/us/en/pages/risk/articles/managing-vendor-risk-in-extended-enterprise.html

4| Make sure vendors meet their industry standards and document it

To ensure vendors provide appropriate security, controllers and processors in relation to their sub-processors should exercise pre-contractual due-diligence through methods such as RFIs/RFQs, site visits and audit observations. This step can very well build on step Two's collaboration with the Security teams and steps Three's VRM principles. The privacy considerations that are examined can include the following[20]:

i. Processor's data protection knowledge and awareness.

ii. Recent high-profile breaches on the processor's side and mitigation steps.

iii. Is the processor currently undergoing any regulatory investigation or audit, including its potential cause and focus?

iv. Any accreditation, certification or codes of conduct.

v. Processor's policy framework.

vi. Sub-processors currently employed by the processor, and their respective location, measures to safeguard the processing etc.

British ICO provides a checklist for security assessment. It also recommends "cyber essentials" baseline set of controls – firewalls, secure device settings, access controls, anti-malware, and software updates — as a "good starting point," and then building a program out from there depending on the organization's particular circumstances and risks.[21]

French CNIL's guidance outlines the basic precautions that organizations should take security-wise:

i. Listing the processing of personal data, the data processed, and the media on which they rely.

ii. Assessing the risks generated by each processing operation.

iii. Implementing and checking the planned measures.

iv. Carrying out periodical security audits, with each audit producing an action plan "monitored at the highest level of the organization."[22]

---

20 IAPP Article containing more detailed notes on implementing appropriate security under the GDPR: https://iapp.org/news/a/implementing-appropriate-security-under-the-gdpr/

21 ICO Security guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/ ICO Information Security Checklist: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/information-security-checklist/

22 CNIL Guide of Personal Data Security (in French): https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

In addition to regulatory guidance, there is also a number of pre-existing information security frameworks that can be leveraged. For instance, the IAPP and OneTrust recently published a white paper identifying six main areas of common ground between the ISO 27001 standard and the GDPR, "intended to demonstrate how ISO 27001-certified organizations are well positioned to respond to many GDPR priorities." Although they come from different perspectives, ISO 27001 and the GDPR at their core are both about reducing risk to people and organizations caused by misuse of personal data, with demonstrable overlap in both principles and requirements.[23]

Furthermore, the Cloud Security Alliance (CSA) established a widely recognized CSA Consensus Assessments Initiative Questionnaire (CAIQ) framework that helps to provide commonly accepted industry standards to document security controls in Software-as-a-Service, Infrastructure-as-a-Service and Platform-as-a-Service applications. The CAIQ was designed to help with one of the leading concerns that companies have when moving to the cloud: the lack of transparency into what technologies and tactics cloud providers implement with regards to data protection and risk management, and how they implement them. The CAIQ questionnaire can be customized to suit the requirements of each cloud customer and used to help organizations build the necessary assessment processes for engaging with cloud providers. The CAIQ is intended to be used in conjunction with the CSA Cloud Controls Matrix (CCM) and the CSA Code of Conduct for GDPR Compliance. The latter was created by industry experts and representatives from the EU's national data protection authorities to help companies adhere to the EU's GDPR data privacy regulation. The CSA's Code includes all the requirements a cloud service provider must satisfy to comply with the GDPR.

OneTrust is a strategic partner of CSA and the OneTrust Vendor Risk Assessment module contains the CSA CAIQ, CCM, and GDPR code of conduct templates in a number of language variations for operations in local markets.[24]

On a similar note, many companies may find it practical to employ the SIG shared questionnaire as a tool for risk management assessments of privacy as well as data security, cybersecurity, or IT business resiliency. SIG uses large number of questions from a spectrum of domains (risk control areas) for determining how security risks are managed within a service provider's environment. SIG can be used to evaluate service providers' risk controls, or even can become a helpful RFP response element. However, some companies even rely on SIG for self-assessment.

---

23 Please see the IAPP article for more details on the overlaps between GDPR and ISO27001: https://iapp.org/news/a/gdpr-compliance-combine-and-conquer/ IAPP-OneTrust Research: Bridging ISO 27001 to GDPR available here: https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/

24 Article: OneTrust and the CSA Announce Strategic Partnership https://www.onetrust.com/company/news/press-releases/onetrust-cloud-security-alliance-csa-strategic-partnership-privacytech/

SIG is also fairly scalable as its scope can be determined on varied levels of detail. Some companies may choose to use 'SIG Lite' assessments for broad high-level assessment of internal information security controls (for example as a preliminary assessment tool), whereas others will prefer to employ the full SIG assessment version. OneTrust Vendor Risk Assessment module supports both the SIG and SIG Lite assessments.

Additionally, there is significant overlap in privacy vendor assessments with the AICPA Trust Service Criteria, which serves as the basis for the popular SOC 2 report. Other helpful frameworks include the NIST 800-53, COBIT 5.0, and ENISA IAF.

Although not specifically tailored to the GDPR, these frameworks are still relevant as they have been well-respected and have served as industry-standards for many years and can be immensely valuable as part of establishing your overall security posture.

Documenting

Given that the GDPR is very much focused on accountability and demonstrating compliance, it comes naturally that every vendor-review (and generally compliance) step and finding should be documented. It is very important to document the audit/ review process and its outcomes, especially upon assuring that the vendors meet the established privacy and security requirements.

5| Establish vendor review cadence

Vendor Name
Vendor Number
Active Status
Application Provided
Last Audit Date
Complience Reports

For effective vendor risk management, it is important to correctly set up a vendor review cadence. Frequency of vendor reviews would likely differ among vendors depending on the risk level associated with each vendor and their processing operations. It may be helpful to set up several vendor review frequency groups for each risk level.

It is also good to remember that a vendor's risk level would elevate if the same risks are detected with the vendor repeatedly during security and privacy audits without being addressed.

Other issues that may affect the vendor review cadence are the contract lifecycle events, such as the contract termination, renewal and substantive amendments of the processing services' scope. All of these may require adjustments in the vendor review timing.

Vendor reviews may need to be embedded or aligned with the internal organization policies, particularly with the existing regimes of annual reviews and similar processes already in place. For those seeking further guidance, the British ICO has come up with Vendor Contracts Guidelines.[25] Furthermore, it may be worth seeking the opinion and advice of the lead Data Protection Authority on certain related issues.

The scope of vendor review should include all the active vendors. It is still important to distinguish the personal data processors amongst them (likely a majority) and rank those accordingly in terms of risks. Make sure to include all the active vendors in your ERP (Enterprise Resource Planning) /SCM (Supply Chain Management) Systems – you can still distinguish between them based on the associated risks and thus prevent any audit overburdening. Also, do include your service or application providers from your data inventory, some of those will likely be in potentially higher-risk data processor roles.

---

25 British Information Commissioner's Office draft guidance: GDPR – Contracts and liabilities between controllers and processors, available here: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf

6| Embed privacy structure into your vendor reviews

NEW VENDOR REQUEST PROCESS	Embed Privacy Reviews in Procurement Process
CONFIGURATION MANAGEMENT DATABASE (CMDB) EVENTS	Embed in Contract Renewals and Vendor Updates
GRC FEEDS	Integrate Vendor Risks into Overall GRC Framework

While the general notion of involving privacy teams in vendor vetting and processor audits is fairly straightforward, in practice many organizations find it quite difficult for the Privacy teams to be informed about the key operations and project stages at the exact time when they should be stepping in. This in turn causes frustration and delays for the teams. A good way to tackle this issue is to focus on key "privacy triggers" within the existing company processes. Here are some examples:

i. New Vendor Request process – consider where within the existing company procurement process the privacy team's vendor review should be triggered. Update the checklist on vendor onboarding steps to include the notice to Privacy team in a given stage.

ii. Configuration management database (CMDB) events – whenever a data warehouse or IT inventory installations are due, this should likely trigger privacy and security vendor review in the earliest stages. Embed these triggers in contract renewals and vendor updates, so that they are tied in with these contracts' lifecycles.

iii. GRC Feeds – As was already mentioned, the privacy vendor assessments will be more efficient (and less burdensome for your operations) if in synergy with existing frameworks. The Governance, Risk and Compliance framework that already exists within your organization would in turn benefit from the additional layer of privacy vendor review and aligned vendor risk assessments. As the vendors are often already monitored for certain performance measures, like financial, relationship and compliance, it makes sense to align the additional privacy monitoring with these too.

7| Update data processing contracts and vendor records

PRIMARY VENDOR: COORDINATE TERMS AND RESPONSIBILITIES

Review Transfers (Privacy Shield, Model Clauses)	Security Commitments	Requireent to Assist in Responding	Liability and Risk Coverage	Data Breach

Probably one of the most time-consuming exercises under the GDPR is the review and renegotiations of the existing data processing agreements with the processors. Make sure that all the existing processor relationships are governed by contracts that include all of the GDPR Art. 28 requirements (please refer to "Section E: Contractual Terms" of this Handbook for more details on the requirements).

The review of existing processor contracts should also include review of all the existing sub-processors and checking that controller is aware of any updates in these relationships. Furthermore, existing personal data transfers outside the EU/EEA (both on the side of processors and sub-processors) should be reviewed – e.g. by checking that the company Privacy Shield certifications are still up-to-date. As the renegotiation of certain provisions in existing data protection agreements can become quite time-consuming and often contentious issue, it is reasonable to divide the processors into risk-based groups and prioritize the negotiations accordingly.

Other obligations of controllers and processors (e.g. record-keeping, ensuring the security of data processing, etc.) will still apply in addition to any contractual obligations which a controller and processor may be subject to under a data processing agreement. It may helpful to ensure that especially smaller organizations entering into the data processing agreement are aware of their new GDPR obligations, as this may prevent some potential issues affecting the other contractual party in the future.

It is also good to remember that besides the contractual liability, the controllers and processors can become liable to regulatory fines and other public-law penalties under the GDPR separately, aside from any contractual damages and liabilities. The data protection agreements should not therefore try to copy the existing statutory liabilities, but rather should only focus on the contractual relationship and potential limitation of liability between the parties based on this relationship alone.

8| Determine integration and synergy areas

Procurement	Contract	GRC	PM Tools	ITSM
SAP Ariba	ORACLE	servicenow	JIRA	bmc Remedy
ORACLE	coupa	ARAVO	SharePoint	servicenow
mercateo		R-sam		
		RSA Archer		

On the operational level, instead of starting vendor risk management from scratch, the organizations using enterprise can take advantage of the existing systems and vendor information by integrating them with the privacy & security vendor risk assessments. It is therefore worthwhile to look for vendor risk management software that enables integration with the software already used by the company for procurement, asset inventory, project management etc. By integrating these tools, the company can save itself a large amount of resources otherwise spent on populating vendor risk assessments with already existing information and trying to keep those up-to-date manually.

Here are some areas of company operations which are likely to render data for vendor risk management and should thus be considered for integration of software systems: HR, Logistics, Financial Management, Cash, Accounting, Asset Management, Project Management, Maintenance.

9| Formalize management of risk

With the GDPR the privacy law has become much more concerned with risk assessments, risk mitigation and risk management than ever before. For the Security teams and perhaps other business-related teams within the company, the management of risk is not a new discipline. However, with the legislative backdrop and accountability principle being now present, the organizations need to establish or expand their program management to operationalize the risk management while still complying with the need to demonstrate and document the company's steps.

There are some practical ways how to achieve this:

i. **Organize** – Make vendor risk assessment a key discipline within the company, involving members of various teams will ensure easier synchronization of the company operations' as well as better recognition of each team's concerns and priorities related to the vendor management.

ii. **Train** – Make sure that the vendor acquisition team is aware in more detail about the requirements of the vendor management process. At the same time, all staff must be aware on a high level of the vendor management processes and relevant outcomes for them. Make effort to involve Marketing or PR teams in the training to ensure, that the message is presented to the employees in an easy, less legalese language – ensuring it's accessible to all the employees.

iii. **Quantify Risk** – Use a consistent and standardized approach to risk assessment. It should be flexible enough to cover various types of risk and still comprehensive enough to be correctly used by employees without Privacy or Security background. Typical elements determining risk can be volume of personal data processed, sensitivity of the data, timelines of processing, technical parameters of the processing etc.

Risk	Project Name	Risk Description
	Vendor IT Risk Assessment	You should never use plain-text protocols for remote device administration and management. These protocols should use encrytion to protext credentials passing over the network, and they should also protext the integrity of the transmitted commands in order to guard against manipulation.
	Vendor IT Risk Assessment	Using this authentication method without at least a username and password is highly unusual. Did you forget to check the "Usernae and password" box?

iv. **Automate** – Building automation into vendor assessment can be a significant help to identify risks, indicate further questionnaires are necessary, and automate risk recommendations and status updates. With the right technology platform in place, your organization will have overview of your vendor management network and should be more confident in tracking any development and measuring vendor milestones. Simultaneously, you will be automatically generating documentation demonstrating your compliance with the GDPR.

10| Establish a vendor risk management lifecycle

Most of the previously mentioned steps should (once implemented) form together a framework fitted to the operations of your organization. It is ideal, if you can synchronize all these vendor risk assessment tasks and operations into a vendor risk management lifecycle. On practical terms, this can be done through the following steps:

i. **Standardize vendor audits** – establish a standard version of desktop audits, in-person audits, third-party reports, certifications and standards.

ii. **Track risks** – establish due diligence review including preparation of risk ratings and findings, which will in turn save a lot of time and limit confusion when using the framework by the employees in the future. Furthermore, require remediation by the vendor or business unit: risk-rate and prioritize vendors, actively monitor them, escalate if timelines are not met.

iii. **Document communication** – as is the golden rule of accountability under the GDPR, documenting of vendor audits should include also related internal and external communication. Particularly internal communication between the privacy team and business owners, or external communication to the vendor can be useful for demonstrating compliance.

iv. **Review vendor reports** – vendor reports need to be frequently reviewed – either based on any changes to the relationship (termination, change of services) or as a part of periodic assessments and audits. Any new findings must be reflected in vendor reports, in order to maintain these up-to-date.

v. **Re-audit vendors periodically** – it is important to embrace that vendor audits are not a one-off exercise in the beginning of the relationship. On the contrary, the audits should be conducted periodically to help you ascertain any changes on the vendor side that might pose risks. Aside from the periodical audits, vendors that have experienced high-profile data breaches or that have otherwise raised concerns about their privacy and data management practices may need to be re-audited in response.

Reference

- Key GDPR Articles for vendor risk management
- Article 4(7) and 4(8): Definitions of Controller and Processor
- Article 24(1) & Recitals 74-77, 83: Responsibility of the Controller
- Article 26 & Recital 79: Joint Controllers
- Article 28 & Recital 81: Processor
- Article 29: Processing Under the Authority of the Controller or Processor
- Article 32 & & Recitals 74-77, 83: Security of Processing
- Article 45 & Recitals 103-107: Transfers on the basis of an adequacy decision
- Article 46 & Recitals 108-109: Transfers Subject to Appropriate Safeguards
- UK ICO guidelines: Consultation: GDPR guidance on contracts and liabilities between controllers and processors, Information Commissioner's Office (consultation period: 13 September 2017 – 10 October 2017).
- Ireland DPC guidelines: Guidance: A practical guide to data controller to data processor contracts under GDPR, Data Protection Commissioner.
- European Commission Website containing up-to-date list of adequacy decisions: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Repository of Privacy Shield certified companies: https://www.privacyshield.gov/list
- Current forms of EU Standard Contractual Clauses at the European Commission website: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
- Information on Public International Agreements involving personal data where the EU is a party (European Commission website) https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en
- IAPP Sample Data Processing Agreement. Resource: https://iapp.org/resources/article/sample-data-processing-agreement/; See also template from DLA Piper https://iapp.org/resources/article/sample-addendum-addressing-article-28-gdpr-and-incorporating-standard-contractual-clauses-for-controller-to-processor-transfers-of-personal-data/

Reference Continue

- Bavarian Data Protection Authority (BayLfD) Guidance AKI 6 on additional costs for GDPR audits (in German): https://www.datenschutz-bayern.de/datenschutzreform2018/aki06.html
- Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" https://www.pdpjournals.com/docs/88016.pdf
- Irish DPC online guidance on determining the "controller" or "processor" role: https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm
- Overview of Vendor Risk Management (VRM) term: https://www.gartner.com/it-glossary/vendor-risk-management.
- Practical use of VRM with technology: https://www2.deloitte.com/us/en/pages/risk/articles/managing-vendor-risk-in-extended-enterprise.html
- OneTrust article talking about proper security measures https://iapp.org/news/a/implementing-appropriate-security-under-the-gdpr/
- ICO Security guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/
- ICO Information Security Checklist: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/information-security-checklist/
- CNIL Guide of Personal Data Security (in French): https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- IAPP-OneTrust Research: Bridging ISO 27001 to GDPR available here: https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/

OneTrust

Privacy Management Software

About OneTrust

OneTrust is the largest and most widely used dedicated privacy management technology platform for compliance with global privacy laws. More than 1,700 customers, including 200 of the Global 2,000, use OneTrust to comply with global data privacy regulations across sectors and jurisdictions, including the EU GDPR, ePrivacy (Cookie Law), California Consumer Privacy Act (CCPA) and more. An additional 10,000 companies use OneTrust's technology through a partnerships with organisations such as the International Association of Privacy Professionals (IAPP), the world's largest global information privacy community.

The comprehensive platform is based on a combination of intelligent scanning, regulator guidance-based questionnaires, automated workflows and developer plugins used together to automatically generate the record keeping required for an organisation to demonstrate compliance to regulators and auditors. The platform is enriched with content from hundreds of templates based on the world-class privacy research conducted by our 300+ in-house certified privacy professionals.

The software, available in 50+ languages, is backed by 27 awarded patents and can be deployed in either on the cloud or on-premise.

OneTrust helps organisations implement global privacy requirements, including Data Protection by Design and Default (PbD), Data Protection Impact Assessments (PIA/DPIA), Vendor Risk Management, Incident and Breach Management, Records of Processing (Data Mapping), Consent Management, Cookie Consent, Data Subject Rights, as well as demonstrating accountability and compliance.

PrivacyConnect, OneTrust's user community, hosts free workshops in 85 international cities, and is attended by thousands of privacy professionals to share best practices.

PrivacyTECH, OneTrust's global user conference, occurs annually in London. OneTrust PrivacyTECH brings together privacy professionals to breakdown the latest technology innovations driving global privacy compliance.

OneTrust is co-headquartered in Atlanta, GA and in London, UK, with additional offices in Bangalore, Melbourne, Munich and Hong Kong. The fast-growing team of privacy and technology experts surpasses 500 employees worldwide.

To learn more, visit OneTrust.com