Navigating supply-chain compliance & cloud Risk

TRACE DATA COMPLY GUIDES

'Navigating Supply chain Compliance and Cloud Risk' Trace Data Ltd., United Kingdom, April 2020

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/eli/reg/2016/679/oj

“

The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures

-Article 28, the GDPR

”

OVERVIEW

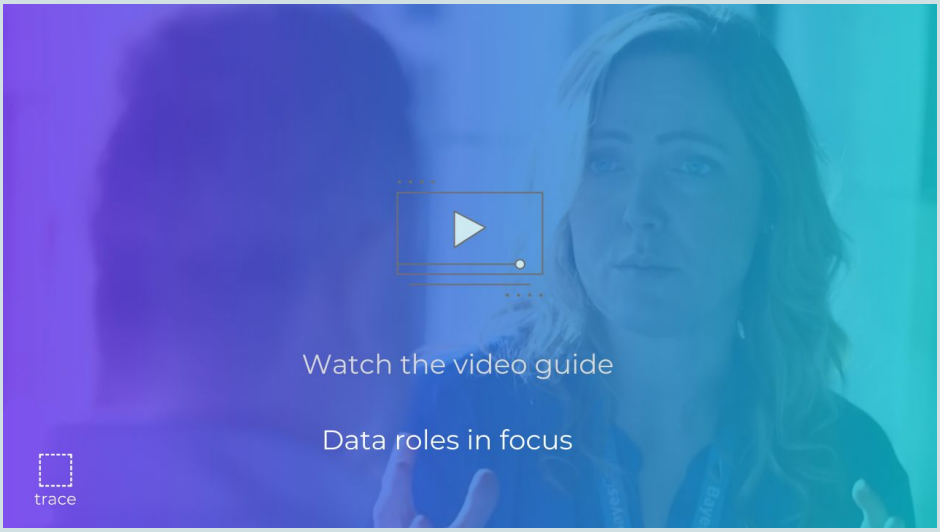
Complying with regulations like the General Data Protection Regulation (GDPR) is complex but vital for data-driven, responsible organisations. Privacy is an ongoing, multifaceted and risk-based programme, and one which needs to be based on 'Accountability' and upholding principles like Privacy by Design, to be sustainable.

In this guide we'll explore one of the essential aspects of compliance: working with trusted data processors. We'll look at your compliance responsibilities and potential risks when it comes to the partners, cloud services and vendors you share personal data with. This guide is aimed at organisations who need to comply with the GDPR, who process personal data of European citizens (as 'data controllers').

Roles and responsibilities

Let's start by understanding key data roles when it comes to compliance and your suppliers, as a controller. Our video explains data roles in the context of Data Protection regulations like the GDPR.

Click the image to play the short video overview.



Assuring your suppliers

Simply put, if you share personal data of data subjects (such as your clients or employees) with your suppliers, service providers or cloud vendors, you need to check your chosen partners will protect that information and be trusted custodians.

As a controller, you have an obligation to assure your data processors and protect your organisation from privacy and third party risk with the right legal agreements with processors and sub processors. Such due diligence or assurance is part of your responsibilities under the Accountability principle, but it's also a question of best practice and protecting your organisation from risk, contract gaps and liabilities.

> **The controller shall be responsible for, and be able to demonstrate compliance with...'accountability'**
>
> -Article 5(2), the GDPR

The five GDPR articles in focus for you to ensure your Data Processors uphold:

- (Article) 28, requires **contractual protections** with processors and their sub-processors, adequate data protection, and evidence of their compliance with the GDPR
- 30, requires data processors to maintain an **inventory** of the personal data they host
- 32, data processors and their sub-processors are required to to implement robust **security** controls to protect personal data
- 33, data processors required to report on breaches to clients 'without undue delay'
- 36, processors should provide Data Protection Impact Assessments (DPIAs) to their clients in certain high-risk scenarios.

Who do you share your data with?

Electronic data: it gets everywhere; it's hard to track through its lifecycle and can be easy to leak. Digital information certainly makes its governance a challenge, and an important one - especially when it comes to personal and high risk information like medical or financial, which needs extra care.

So where does data flow in your organisation? Undertaking the audit and maintaining your (Article 30) inventory, (whether manually, or with the help of applications like Trace), helps you understand the where's and who's of the personal data you process.

Examples of data processors where personal data might be processed:

- ➔ Cloud services your organisation uses, such as Google or Microsoft cloud services, for email or document storage, for example
- ➔ Suppliers such as market research agencies who survey your customers
- ➔ Your HR or Accounting software or partners: handling your employees' information.

CAVEAT EMPTOR

Assuring your third parties

When it comes to your partners and data processors, be aware that they can often be the source of breaches, so choose them wisely and assure them with care, collating and validating evidence of their compliance. Part of your compliance programme should include regular vetting of your existing supply chain, carrying out due diligence on new partners and reviewing contracts.

The average time to identify a breach in 2019 was 206 days

-IBM

And if the worst should happen, you will need to be alerted and ensure your contracts are clear on liability — so no assumptions. Therefore, when you engage data processors, it's important to contractually establish their service levels for assisting with responses to data subject rights requests.

Get things in writing

It is essential to have things written down and legal so that both parties understand their responsibilities and liabilities, and to protect organisations if things go wrong.

DPAs in focus

Which leads us nicely to look at Data Processing Agreements, also known as Data Processing Addendums (DPAs).

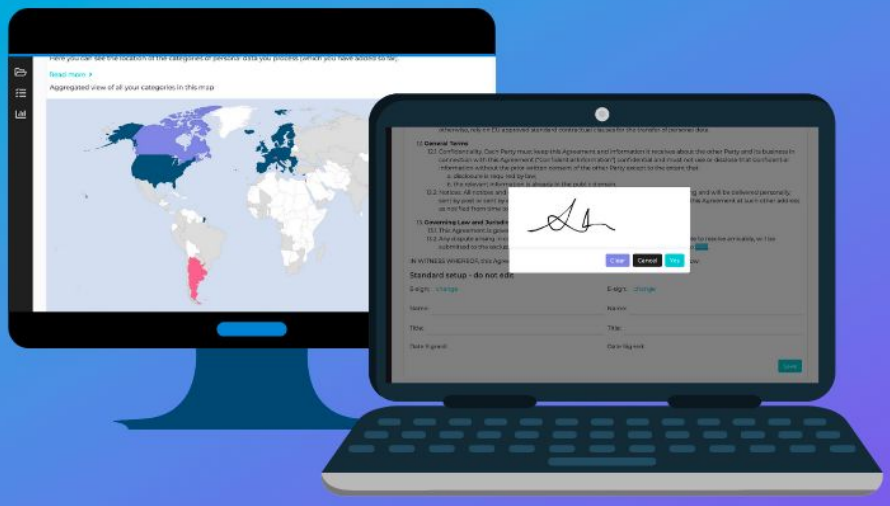
Under the GDPR when as a controller you use a data processor, you need a written contract. If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, they in turn need to have a written contract in place with that sub-processor.

How Trace can help

Trace's app can help you uphold compliance and privacy risk management when it comes to your data processor services, partners and third parties.

Explore our app's features:

- ➔ Trace's smart DPA: allows you to utilise our DPA or build and customise every aspect of your company DPA. You can then e-sign the agreement, note relating contracts and securely share your agreement with your partner for counter signature. All stored in app, or export to pdf
- ➔ With Trace's streamlined processor, you can assess your vendors' compliance posture in app and track and evidence responses to key questions on their data security
- ➔ Trace's in app Data Protection Impact Assessment (DPIA) helps you risk assess projects and partners where data is being processed, and critically log outputs for compliance
- ➔ Global Insights: Trace's unique global data residency tool lets you track global data protection regulations: you can see if your cloud vendors' data centres are located in 'adequate' jurisdictions or whether you need to look at transfer mechanisms. Our app helps you navigate international data transfers, and mitigate legal and cloud risk.



Global data insights; Remote compliance smart tools

tracedata.co.uk

trace

SUMMARY

As we have set out in this short guide, working with trusted partners across your supply chain and cloud services is vital to you as an organisation, it's also an essential part of your compliance responsibilities to the regulatory authorities and your stakeholders. When it comes to compliance, you're only as strong as your weakest link so take a holistic and programmatic approach to privacy.

Key takeaways:

- ➔ Work with your team to understand all of the vendors and partners where personal data is shared. This includes any 'shadow IT', where employees are 'bringing their own cloud' to do work tasks where personal data is involved. Uncover and map all of this through the audit and inventory management
- ➔ Compliance is 'show not tell'; get things in writing with relevant contracts, and ensure compliance evidence can be produced
- ➔ Involve procurement: ensure compliance with regulations like the GDPR is part of ongoing supplier management
- ➔ Train and systemise: make your privacy programme embedded with scalable technology solutions like Trace to help you manage processes consistently and train your team to understand their responsibilities.

z

About Trace

We believe human-centred tech, together with great people, delivers good data for everyone. It's brilliant data protection software and services for privacy pros, *by privacy pros*.

Get in touch with Trace

- ➔ Book a free Video Call demo
- ➔ Find out more on our website
- ➔ Email us at info@tracedata.co.uk