Trace your way to proactive risk management

trace®

Enforcement actions are increasing in frequency and severity, fuelled by DPAs' growing power.

Data is a precious resource and processing it is the bedrock of daily business. Ensure data drives reward, rather than risk.

When it comes to data processing risks, the spectre of regulatory censure looms large, and with good reason. The threatened financial penalties are of a magnitude to pose an existential threat to smaller organisations; as fines are proportionate to revenues, even the largest cannot shrug them off.

Between the GDPR's May 2018 go-live and August 2020 European Data Protection Authorities issued 343 fines totalling just over £437 million, but this is very much just the start. For two high-profile cases, the UK's ICO has issued intent to fine notices amounting to £282 million.

Enforcement actions are increasing in frequency and severity, fuelled by DPAs' growing power. The ICO's budget has increased 51% year over year and its staffing by 40%.

Rightfully, given the potential for harm, there is a laser focus on data breaches: almost 300 were being notified to European DPAs every day even before the COVID-19 pandemic led to a 63% spike in cybercrime. Yet what is often underappreciated is that security and breach notifications can actually come under the lower-tier (€10 million/2% of turnover) enforcement regime.
The fines may be harsher still (€20 million/4% of turnover) for failings concerning the lawful bases for processing, consent, data subject rights, international transfers and more.

Higher €10 million/2% of annual global turnover	Higher of €20 million/4% of annual global turnover
Data protection by design and by default	Data Processing principles
Records of processing	Lawful basis of processing
Controller-processor arrangements	Consent
Security	Special category date processing
Data Processing Impact Assessments	Data subject rights
Data Protection Officer	International data transfer

Focus: Processor and Transfer Risk

The requirements for Data Processing Agreements are complex and Standard Contractual Clauses may no longer be enough.

Some 90% of organisations use third party processors and they are estimated to be involved in two-thirds of breaches.

Although processors have responsibilities, liability remains with controllers.

The requirements for Data Processing Agreements are complex and Standard Contractual Clauses may no longer be enough.

DPAs are recommending additional safeguards post Schrems II and international transfers remain under intense scrutiny.

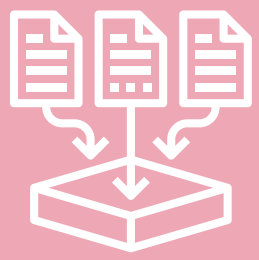
GDPR enforcement actions at end-August 2020

Infringement	Fines Total* at end-Aug 2020/frequency
Legal basis for data processing	£115M/147
Technical and organisational security measures	£300M/80
General data processing principles	£16M/59
Data subject rights	£9M/38
Data breach notification	£200K/9
Data protection officer	£120K/4
Data processing agreements	£13K/2

*rounded, converted

Source: GDPR Enforcement Tracker

Focus: DSR Risk



Data Subject Requests are increasing with privacy awareness. Two out of three organisations handle them entirely manually, and could easily become overwhelmed: already, 44% of receive 1-10 a month and 18% up to 100. Access and erasure are most common (68%/60%), but even these seemingly simple requests can be anything but.

Locating unstructured personal data is a huge pain point. Privacy professionals say entirely manual processes make fulfilling DSRs 38% more difficult than the average – with the result that almost three-quarters of firms are unable to respond "without undue delay", despite over half having a team dedicated the task.

A worryingly high proportion even skirt the one-month deadline.

In contrast, a quarter are able to respond within days or even hours because they have invested in tools to efficiently track and trace data and manage DSRs end to end.

Multi-faceted Risk Exposure

Focus: DSR Risk

Regulations emulating the "gold standard" are springing up all over the world.

And fines are just one element of the potential punishment firms face. Supervisory authorities can publicly "name and shame" wrongdoers, make them submit to onerous oversight or even order them to cease transferring/processing data altogether. Many might not survive such damage to their reputation and revenue.

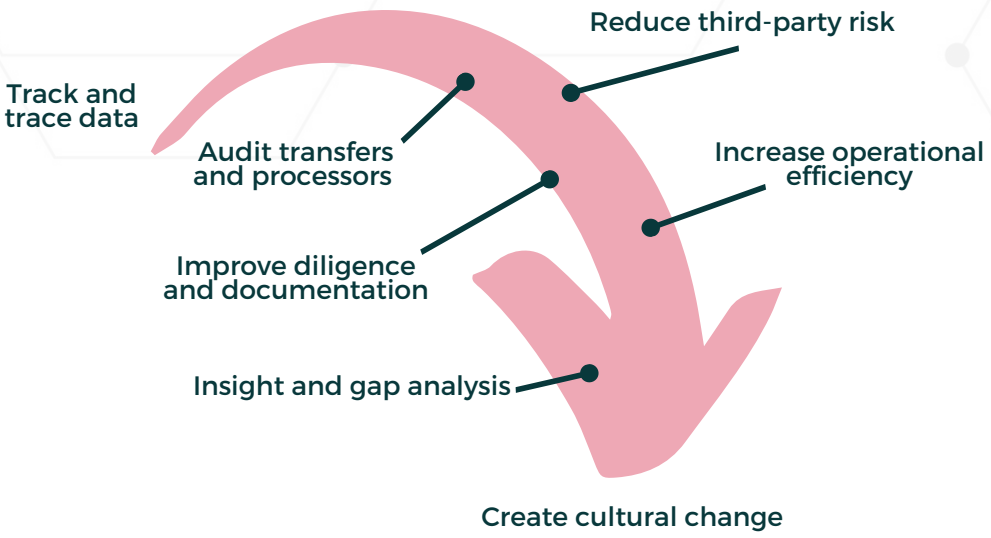
Regulations emulating the "gold standard" are springing up all over the world. Yet more than two years into the GDPR's reign serious compliance gaps remain.

Fewer than half of privacy practitioners report that their organisation is very/fully compliant with its obligations. Include those without such personnel – or the wherewithal to know – the true extent of non-compliance is likely to be very much higher.

Individuals are also empowered to seek compensation, and organisations will have very little defence against these claims where DPAs have already done the work of proving liability.

Representative or class actions are expected rise exponentially: litigation funders with deep pockets have smelt blood in the water.

Proactively Dial Down Risk



Focus: DSR Risk

There is a direct correlation between having a privacy programme and reduced risk of breaches.

Key Trace platform functionality:

- Unique global data visualiser;
- Map data cloud locations against global regulations;
- Audit your transfers;
- Update and track DPAs and third-party assessments
- Expedite supply chain review, mitigate cloud issues.
- Cost-effective, on-demand access to expert DPO Services (RoPAs, DPIAs, LIAs, data governance frameworks etc).

There is a direct correlation between having a privacy programme and reduced risk of breaches. Getting a grip on your data and operationalising compliance creates real cultural change.

A chasm is opening up between organisations which have correctly weighed the risks (and rewards) at stake, and those prepared to dance with danger. Ensure you are on the right side of the divide.

GDPR Enforcement tracker
DLA Piper GDPR data breach survey: January 2020
Ibid
"The Impact of the COVID-19 Pandemic on Cybersecurity" ISSA/ESG
Annual IAPP Privacy Governance Report 2019, IAPP-EY IAPP-EY Annual Privacy Governance Report 2019

trace®

Want to know more?

www.tracedata.co.uk

Edinburgh:
Bayes Centre, 47 Potterrow,
EH8 9BT, UK

New York:
9th Floor, 524 Broadway,
New York, NY, USA