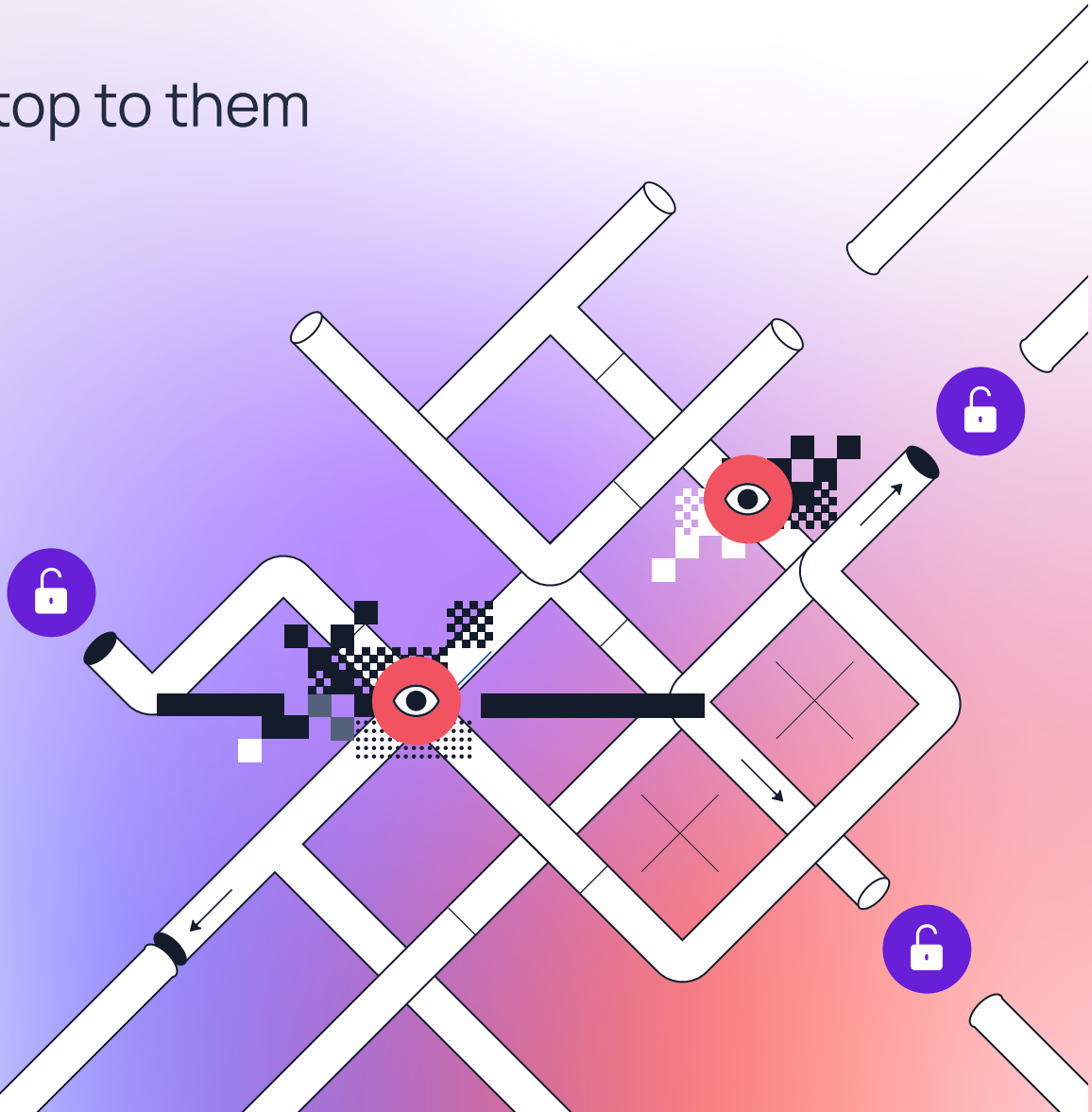
soveren

Privacy violations

Put a stop to them



Privacy violations: put a stop to them

Data usage internally and with third parties is necessary for all businesses to operate, but without strict controls and monitoring of what data is shared with whom and for what purposes, companies can find themselves falling short of safeguarding personal data or complying with privacy regulations like GDPR.

deel.

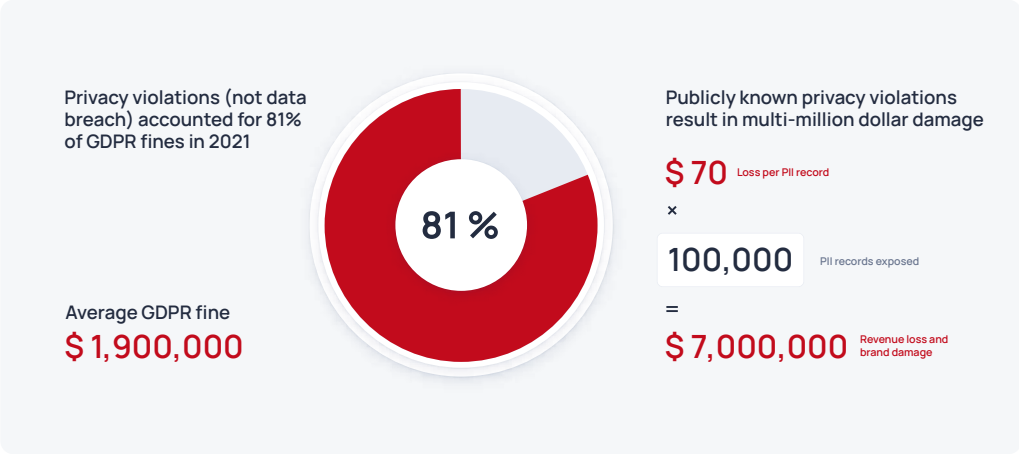
Frankly, privacy is no longer a question of just GDPR or CCPA compliance. Privacy incidents damage your brand, growth, and ability to attract capital. With Soveren it just got easier to protect yourself from privacy incidents and risks.

Alex Bouaziz
Co-Founder & CEO at Deel

This is because there is a huge privacy void between the legal measures and security software which most businesses rely on when it comes to personal data. There are two reasons for that:

- Legal measures alone can't guarantee compliance — even the best privacy policy is just a piece of paper that doesn't protect personal data from being exposed
- Security software (like NGFW or DLP) successfully addresses security threats, but has a limited impact on addressing privacy challenges because — unlike other confidential data that can be easily isolated and sealed — personal data is actually meant to be accessed, used, and shared in-day-to-day business operations

Privacy violations that make headlines result in multi-million dollar revenue losses and brand damage. In fact, every single PII record lost costs organizations $70, meaning an event which exposes hundreds of thousands of records can have a detrimental impact in the millions of dollars.



Besides the reputational damage of inadequate personal data protection, over 10M businesses globally are at risk of violating privacy regulations. Privacy violations expose your business to risks of revenue loss and regulatory fines averaging $1.9M.

But what are privacy violations, and how can we prevent them?

Main types of privacy violations

Privacy violations can be grouped into different categories, related to:

- Infrastructure misconfigurations
- Events
- Data lifecycles

In addition, there are also two categories that need to be constantly monitored to detect and prevent data exfiltration which leads to privacy violations:

- Anomalies
- API configurations

Below are handy tables about the different types and violations within each category, including a description of the consequences and advice on how to prevent them.

1 Source: Soveren analysis based on public information.

2 Source: GDPR Enforcement Tracker, September 2018 – March 2022.

Infrastructure misconfiguration

Incorrect infrastructure setup can lead to data leakage or over-sharing, data being stored where it shouldn't be digitally (i.e. in persistent storage or logs) and physically (in line with data localization laws).

Privacy violation	Example	Consequences	How to prevent
Legitimate 3rd-party service gets more information than described in DPA	3rd-party vendor has access to more personal data from your company or you receive more PII from contractors than stated in the contract	Fines and supply chain attack (data stolen from the vendors infrastructure) GDPR articles violated: 5, 28, 46	Continuous control of data in motion
Cross-border transmission (national border)	You transfer customer PII to other geographies without expressed consent to do so	Fines GDPR articles violated: 46, 49	Data localization by jurisdiction, control over data flows
PII in persistent storage (logs that you can't subsequently delete)	You record application logs into long-term backup systems and PII ends up in these logs	Fines GDPR articles violated: 5, 32	Internal auditing of the logs and development project to change the log structure or obfuscation of data in logs
Transmission of health data	You don't know you have been collecting highly sensitive health data that requires additional protection	Fines and increased severity from the consequences of a data breach brand reputation damage GDPR articles violated: 9, 32	Maintain complete data inventory, prevent disclosure of health data to third parties
Payment data outside of designated environments	You have data vaults for payment data but it isn't only stored there and is processed by other systems	Fines GDPR articles violated: 5, 32 PCI DSS violated	Complete data inventory, code review, and internal audit

Privacy violation	Example	Consequences	How to prevent
Exact geolocation coordinates are collected	You collect geolocation coordinates from your customers	Fines GDPR articles violated: 5, 6	Complete data inventory, code review, and internal audit
Data collected from public sources	Your product collects data including identifiers used by social networks (which could be construed as profiling)	Fines GDPR articles violated: 5, 6, 13, 14	Complete data inventory, code review, and internal audit
Social security numbers present in systems	You collect social security numbers but aren't aware of this	Fines GDPR articles violated: 5, 6	Complete data inventory, code review, and internal audit
Uploads of locally processed data	You built a separate environment for passport numbers or payment data but you aren't sure that this data hasn't found its way to storage elsewhere	Fines GDPR articles violated: 5, 6, 32	Complete data inventory, code review, and internal audit

Event

Events are about changes that are taken that have an impact on your privacy posture. For example, if your marketing team makes changes to the PII that they are collecting from potential clients and that involves collecting data not outlined in your policies (for example, age), this event could be a privacy violation.

Events also include recurring actions such as when systems exchange risk scores about users.

Privacy violation	Example	Consequences	How to prevent
New PII data type in the company environment	Product team adds a new feature, meaning the product begins to gather additional data types	Fines GDPR articles violated: 5, 6, 13, 30	Include privacy people into the design phase of every new feature internal development and implement data flow controls
New PII data type for particular service	You have two different products within one company and allow product 1 to extract data from product 2, giving excessive access to data than expressed in the DPA for product 1	Fines GDPR articles violated: 25, 28	Include privacy people into the design phase of every new feature or changes with data
New service which consumes PII	Creation of a new service or product to existing portfolio and decide to use PII from existing products/services	Fines GDPR articles violated: 5, 25	Include privacy people into the design phase of every new feature or changes with data
New sensitive data type in the company	Your company collects data on gender and location which violates your privacy policy	Fines and brand reputation damage GDPR articles violated: 5, 9, 13	Continuous data inventory: an understanding of what data your different services collect
Privacy policy outdated	Your privacy policy doesn't reflect all the data gathered from users or the data scenarios that the data is used for	Fines GDPR articles violated: 13	Review all usage scenarios for the data that you have in your infrastructure and review your privacy policy frequently

Potentially vulnerable configurations	Example	Consequences	How to prevent
Single request with a lot of data subjects	Request for a lot of data subjects from a one API call, e.g. we have an API that makes requests for UID 123: but an issue in the API means it returns PII on all UID's beginning with 1	Potential risk of data breach and potential fines GDPR articles violated: 25, 32	Complete data inventory, code review, and internal audit
Profiling and risk-assignment	You carry out profiling of customers such as automated credit check and issuance	Potential fines GDPR articles violated: 5, 6, 13, 14	Review all usage scenarios for the data that you have in your infrastructure

Data lifecycles

These privacy violations concern your approach to data operations, including the processes and practices that you have in place to ensure compliance with data privacy regulations. Here we are talking about gaps in your data privacy setup which leads to, for example, data not being deleted on time or relevant documentation becoming outdated.

Privacy violation	Example	Consequences	How to prevent
Personal information wasn't deleted in accordance with retention schedule	You face conflicting regulations and don't understand what data you should delete in line with retention rules	Fines and loss of data consistency GDPR articles violated: 5, 25, 30	Check the data you are storing and delete outdated data
Personal information wasn't corrected upon request	You receive a request to amend data in line with DSAR	Fines GDPR articles violated: 16	Keep data inventory up to date and have a process for data correction
Data deletion job not triggered in production	Your process to run a data deletion job in production wasn't executed due to technical issues	Fines GDPR articles violated: 5, 6, 17	Need to monitor data deletion job via log analytics; have specific rules which are triggered when something goes wrong with the data deletion job
Data update job not triggered in production	Your process to run a data update job in production wasn't executed due to technical issues	Fines GDPR articles violated: 16	Need to monitor data update job via log analytics; have specific rules which are triggered when something goes wrong with the data update job
Data inventory / data map outdated	You created your data inventory last year and haven't kept track of any changes	Fines GDPR articles violated: 25, 30, 32	Frequent (quarterly based) review of data map and data inventory
Risk assessment outdated	You carried out a DPIA, but have added new services since doing so	Fines GDPR articles violated: 32, 35	Frequent (quarterly based) review of data practices and reassessment when new processes are added

Anomalies

Anomalies are different to the above categories in that they do not involve violations to privacy per se, but rather need to be tracked to detect and prevent data exfiltration which leads to privacy violations. Anomalies involve one-time actions such as a single request which exposes multiple PII records or when unexpected datasets containing PII are sent or received.

Privacy violation	Example	Consequences	How to prevent
Increased volume of requests in a single API	You had 10 requests to the API yesterday but today this API receives 10,000 requests	Anomaly that can be a sign of data breach	Apply firewalls or API gateway logs to monitor activity and see when request amounts spike
Increased volume of requests by a single consumer	You have a 3rd-party or internal service that requested 3 APIs containing personal data, today the service requests PII from all the APIs containing it	Anomaly that can be a sign of data breach	Apply firewalls or API gateway logs to monitor activity and see when API request spike

API misconfigurations

Misconfigurations of APIs can lead to privacy violations since they can cause you to share too much customer PII out of the scope of your data protection agreement or expose personal information to publicly accessible data sources. It is important to monitor what data APIs are requesting and accessing because a misconfiguration could lead to a full-scale data breach.

Privacy violation	Example	Consequences	How to prevent
Possibility of single request with a lot of data subjects	Request for a lot of data subjects from a one API call, e.g. we have an API that makes requests for UID 123: but an issue in the API means it returns PII on all UID's beginning with 1	Fines and increased risk of data breach GDPR articles violated: 25, 32	Code review
Lots of different PII in a single field	You have some APIs which can return different data types in the same field (e.g. email, name, passport number, etc. for one field)	Fines and increased risk of data breach GDPR articles violated: 5, 25, 32	Code review
No authorization is required for API	Support team members can access your customers' financial information	Fines and increased risk of data breach because of wider exposure GDPR articles violated: 5, 32	Control and mapping of PII-usage scenarios outlined as policies
API with PII has access from the internet	You have an internal API which exposes PII that is available publicly online (on the internet)	Fines and increased risk of data breach GDPR articles violated: 5, 32	Control and mapping of PII-usage scenarios outlined as policies
PII data is transmitted through non-encrypted channels	PII is available via http and not https - therefore not encrypted and not secure	Fines and increased risk of data breach GDPR articles violated: 32	Firewalls and network monitoring

Today, CTOs/CISOs struggle to prevent potential violations of internal policies, contracts, and privacy laws. This is because they lack visibility into personal data and its usage or don't have expert knowledge of regulations.

Most violations can be prevented by carrying out internal audits, but to do so without a specialized tool is costly and time consuming.

Soveren identifies personal data, detects misconfigurations that can lead to vulnerabilities and violations, and helps remediate fast with actionable insights by automating visibility into internal data flows and outbound transfers.

Stop wasting time on manual reviews

Soveren replaces error-prone manual oversight with automated data visibility, even in highly fragmented and dynamic environments.

Get precise and up-to-date insights

Our technology monitors data flows and tracks every piece of personal data transmitted between services, applications, and APIs.

Cut through the complexity of data flows, take back control over personal data usage, and fix potential violations with actionable insights to:

- Ensure no personal data misuse falls through the cracks with automated data monitoring
- Protect from reputational and regulatory risks without needing to have expert knowledge of privacy
- Easily mitigate potential violations of privacy policies, DPAs, etc.

Authored by Soveren

Soveren's mission is to empower engineering and security teams with automated detection and remediation solutions to manage personal data protection and compliance risks. We help engineering and security teams implement continuous and automated privacy incident detection and remediation.

Book a demo to see how you can protect personal data with Soveren

Trusted by amazing Engineering and Security teams

deel. PandaDoc THE HOTELS NETWORK NU SKIN JOOM

HUBBLE dayzz HeadsUp Performetry.ai CASH EXPRESS