SureCloud®

# How to apply GDPR to your organization in 10 easy steps

**Oliver Vistisen**
**GRC Products Director**

WHITEPAPER

# Table of contents




**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# Overview

Under the new General Data Protection Regulation (GDPR), organizations face astronomical fines for the most serious of infringements, such as failing to have consent to process customers' data. Organizations cannot afford to ignore the new legislation as failure to comply could damage your business. A survey by YouGov found that if they were forced to pay the maximum fines:

- 71% of UK companies fear they would go out of business
- 21% would need to make headcount reductions.

However, the GDPR shouldn't be about scaremongering; running a business is challenging enough without living in fear that you're being watched every second with huge fines looming over your head. With the appropriate compliance framework in place, you can use the GDPR to your advantage, demonstrating to your customers that you are trustworthy, responsible, and derive added value from the data you hold.

Manage your GDPR compliance effectively and you can:

- Build customer trust
- Improve your brand image and reputation
- Improve data governance
- Improve information security
- Improve competitive advantage

If you're ready to use GDPR compliance to your competitive advantage, it's time to schedule your live demonstration of the SureCloud GDPR Suite.

Start your GDPR project today to demonstrate your commitment to compliance.
Contact us: info@surecloud.com

**Article 83:**

General conditions for imposing administrative fines Infringements shall be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

**“ 61% of organizations see further benefits of remediation activities beyond just compliance. Of those, 21% expect 'significant benefits', including competitive advantage, improved reputation and business enablement.**

**Source: Deloitte GDPR benchmarking survey**


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# The challenge of GDPR compliance

According to a report published by Dimensional Research, only a fifth of UK companies believed they were GDPR compliant when the May deadline hit. More alarmingly, nearly a third (27%) have not yet started their implementation. But the failure to act isn't due to laziness or organizations wanting to ignore the issue - 65% actually view GDPR as having a positive impact on their business. The biggest challenge to compliance is the complexity, or at least perceived complexity, the regulation poses.

**But the GDPR doesn't apply to us**

In the UK there appeared to be a degree of naivety over the GDPR, with a third of businesses feeling the legislation would have no impact on them, and a fifth believing the rules didn't apply to them since they didn't handle consumer data. The GDPR is about more than consumer data. It relates to all information (e.g. employee data, payroll, and pension records), it applies to all types and sizes of organizations (e.g. sole traders, partnerships, PLCs). The bottom line is that no-one is exempt, and we all have a responsibility to achieve and maintain compliance.

**GDPR for U.S. companies**

For companies that are located in the U.S, it seems to be more of a case of confusion over whether the GDPR actually applies to them. According to the GDPR, the European Union (EU) doesn't allow the transfer of its citizens data outside of the country unless the country is deemed to have adequate data privacy laws. In the U.S, only companies that have opted-in to the EU-US Privacy Shield are considered to have adequate data protection.

**But…**

That does not mean these companies are compliant with the GDPR? No, only these organizations have a head-start, making their compliance journey a faster process, requiring less effort. The EU GDPR is a comprehensive piece of egislation, and as such, organizations should not to under-estimate the requirements to demonstrate compliance. When the May deadline hit, just 12% of US organizations were GDPR compliant.

## The GDPR at-a-glance

What is the GDPR: replaces the Data Protection Directive 95/46/EC. It covers any personal data that can identify an individual person. It applies to both automated personal data and to manual filing systems.

When it did come into effect:
25 May 2018.

Where does the GDPR apply:
To any organization that processes, stores or transfers the personal data of EU residents, regardless of whether the organization is based in or outside of the EU.

Who does it apply to:

- Controllers: determining the purposes and means of processing personal data.
- Processors: responsible for processing personal data on behalf of a Controller.

Why has the GDPR been introduced:
to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# How to apply GDPR to your organization in 10 easy steps

## 1. Start with the right people

In the U.S., regulation tends to be more prescriptive, telling you exactly what needs to be done to ensure your compliance. EU regulation is very different. Much of it is left open to interpretation, and so unless you have experience in this field, demonstrating compliance can seem a daunting task.

The first thing to do is get the right people in place. If you don't already have the expertise in-house, you may have to look at training your internal people, or hiring into a new position, such as a Data Protection Officer. If your resources are under pressure, you could consider outsourcing, or how to leverage the power of technology to your advantage.

## 2. Ensure the GDPR is more than a tick-box exercise

There is no simple solution to demonstrating your compliance; you can't just tick a few boxes on a checklist and assume you're done. The new legislation demands that organizations demonstrate compliance with its principles. Therefore, compliance requires you to implement appropriate policies and procedures to protect data, as well as demonstrating transparency and accountability.

Ingrained in the culture of your organization, the GDPR requires involvement and collaboration between all business functions. Compliance is a huge undertaking; there are no short-cuts, so it requires a dedicated budget and buy-in from the right stakeholders, including executives.

## 3. Plan for breaches now

In an ideal world, there would be no data breaches. But whether it's down to a flaw in the process, or human error, mistakes are made. To avoid the huge potential fines imposed by the GDPR, you may need to build new steps into your internal processes to ensure your organization continues to meet the requirements of the regulation.

Furthermore, make sure you have a procedure in place now for reporting any data breaches to the Data Protection Authority. Communicate this procedure to all your employees so they know what to do and ensure there's a process for communicating these incidents to affected customers. Then review your risk assessments so you're certain about how to measure and determine the level of risk to an individual, not just the organization. Thorough preparation puts you in a stronger position going into the new world of the GDPR.


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# How to apply GDPR to your organization in 10 easy steps

## 4. Dedicate more time to consent

The conditions for consent have been strengthened. Now, consent has to be separately documented, with the purpose of the data processing clearly attached to that consent. In most cases, this requires you to change the way you've done things in the past (e.g. opt-in rather than opt-out), and to update the way you store your data so you can prove you have consent. Any required consent prior to the GDPR coming into force will also need to be re-obtained in line with the conditions of the GDPR, if you wish to continue processing the data.

In an attempt to demonstrate compliance, many marketing departments will be busy updating their existing data after executing dedicated campaigns targeted at getting people to opt-in. If your organization hasn't yet done this, have you considered what you're going to do with any data where you don't have evidence of consent? Further consideration must also be given to "special categories" and children, where GDPR outlines specific considerations.

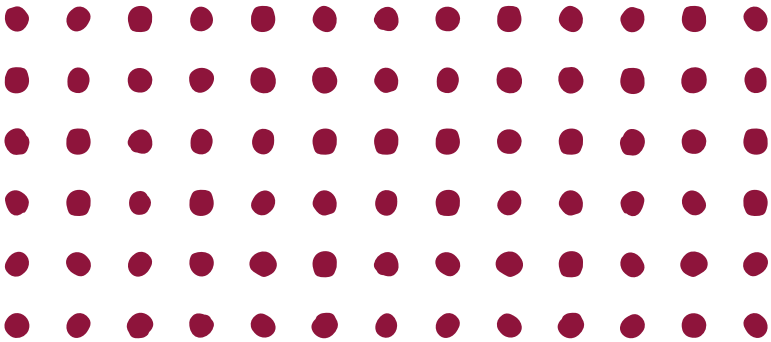
## 5. Enabling the freedom of information

Under the GDPR your customers have rights to not only access their data but also erase or restrict its use, which will require you to have simple mechanisms in place to allow this to happen, without it becoming a burden to your operations.Initially you'll need to verify the person so you are certain the request is from a legitimate source. Then you'll need the ability to identify the data they want, locate where it's stored and act on the request before finally proving you've carried out.

## 6. Don't forget your personal data

A big misconception is that the GDPR is only concerned with customer data. The reality is it covers any personal data that could identify an individual. Think about your internal records and how you store sensitive information relating to your employees. Are you aware of the data you hold? Do you know where it is? And how it's being used? Do you have a purpose for retaining each piece of information? And if/when the data is no longer required, do you have a process for destroying it safely?

Establishing these facts is a crucial first step in your compliance. It may be a simple exercise you can do internally, or you may feel it more appropriateto employ the professional services of an externalagency. In either case, once you know what data you hold, you then need to update your processes for recording, storing and processing this data on an on-going basis to maintain your compliance.




**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

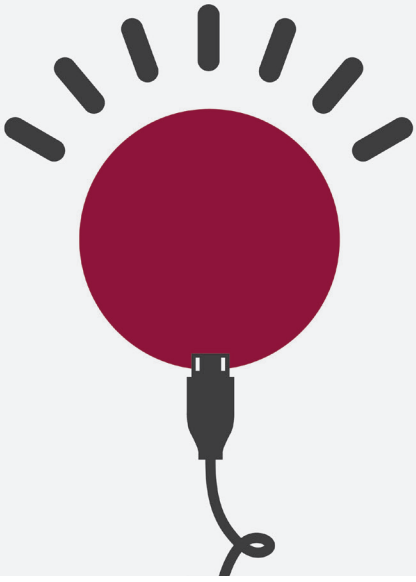
# How to apply GDPR to your organization in 10 easy steps

## 7. Ensure your data protection by design and default

Under the GDPR it's advised that organizations follow 'privacy by design'. This is an approach to programs that ensures privacy and data protection are key considerations in the early stages of any project and continue throughout its lifecycle. Following this best-practice approach is essential for minimizing privacy risks and building trust as any problems are identified earlier, and awareness of data protection is increased more generally across the organization.

### Article 25:

Data protection by design and by default
Implement appropriate technical and organizational measures, which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing.



## 8. Consider your chain of custody

If/when your data is leaving the EU, is this always done directly from your organization, or does it occasionally involve third-parties? And if it's the latter, are they doing it directly, or do they use third-parties? Understanding how your data moves, and who's taking care of it is essential to ensuring it remains protected once it leaves your possession. If you haven't already done so, think about putting contractual clauses in place, and account for your third-parties adequately on your risk assessments.

## 9. Know your responsibilities

The GDPR is very clear about the roles of the person(s) handling data within an organization. In any process you're either a data controller or a data processor, and both roles have important responsibilities to fulfil. Data controllers determine the purposes and means of processing personal data. The GDPR places further obligations on them to ensure your contracts with processors comply with the GDPR. Data processors are responsible for processing personal data on behalf of a controller. The GDPR significantly expands the legal obligations on them (e.g. you are required to maintain records of personal data and processing activities). In the event of a breach, you have legal liability if found to be responsible.

## 10. Leverage the power of technology

This should be used in conjunction with People and Processes, technology exists to make our lives simpler and to help fulfil our compliance obligations. Rather than try to do everything yourself, trust in a dedicated system that reduces the administrative burden, simplifies the GDPR complexity and gives you certainty across your organization that you're always compliant.


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# Introducing SureCloud GDPR Suite

SureCloud GDPR Suite is the simple, effective and structured way for organizations to achieve and maintain compliance. The featured applications in the Suite address all the regulatory requirements that the GDPR contains:

- GDPR Program Tracker
- GDPR Discovery
- GDPR Management
- Information Asset Management
- Risk Management
- Compliance Management
- Incident Management
- Vulnerability Management

Organizations trusting SureCloud GDPR Suite to ensure their ongoing compliance enjoy significant business benefits:

**Cut through the confusion**

Straight out of the box, your Plan-Do-Check project roadmap helps with achieving and then maintaining compliance with the EU GDPR.

**Simplify GDPR compliance complexity**

Organizations should use the SureCloud Integrated Risk Management Platform as a single source for project management, automation, collaboration, tracking and reporting.

**Reduce the pain to achieve and maintain compliance**
Use the auditor-friendly Platform to demonstrate your GDPR compliance program and your ongoing commitment.

**Avoid opportunistic solutions**

As GDPR becomes 'business-as-usual', many compliance tools feeling the strain. Underpinned by the SureCloud Platform, our GDPR Suite integrates with all areas of your organization's GRC.

> **"To address the GDPR, organizations should avoid manual processes encumbered by painful word documents, spreadsheets and emails. Instead, organizations should look to implement a solution/tool that can manage the range and context of the GDPR requirements and processes, to manage compliance consistently and continuously in the context of distributed and dynamic business.**
>
> **Michael Rasmussen, GRC Pundit, GRC 20/20**

Get a free GDPR Suite price quote and demo, plus expert analysis and recommendations to guide your through your GDPR compliance journey.


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# SureCloud GDPR Suite in action

## The GDPR Suite allows organizations to comply with the following articles:

**Article 6:** Lawfulness of processing
**Article 7:** Conditions for consent
**Article 9:** Processing of special categories of personal data
**Article 10:** Processing of personal data relating to criminal convictions and offences
**Article 12:** Transparent information, communication and modalities for the exercise of the rights of the data subject
**Article 13:** Information to be provided where personal data are collected from the data subject
**Article 14:** Information to be provided where personal data have not been obtained from the data subject
**Article 15:** Right of access by the data subject
**Article 16:** Right to rectification
**Article 17:** Right to erasure ('right to be forgotten')
**Article 18:** Right to restriction of processing
**Article 19:** Notification obligation regarding rectification or erasure of personal data or restriction of processing
**Article 20:** Right to data portability
**Article 21:** Right to object
**Article 22:** Automated individual decision-making, including profiling
**Article 24:** Responsibility of the controller
**Article 28:** Processor
**Article 30:** Records of processing activities
**Article 32:** Security of Processing
**Article 33:** Notification of a personal data breach to the supervisory authority
**Article 35:** Data protection impact assessment
**Prior Consultation**
**Article 44:** General principle for transfers
**Article 45:** Transfers on the basis of an adequacy decision
**Article 46:** Transfers subject to appropriate safeguards
**Article 49:** Derogations for specific situations


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**

# SureCloud GDPR Suite

## GDPR Program Tracker

The GDPR Program Tracker starts your compliance journey by asking high-level questions, linked directly to the Articles to visually convey your compliance position. This app uses intelligent, riskbased questions, that also help clarify and prioritize implementation activities as your program evolves. Furthermore, it supports the ability to run multiple gap analysis exercises if required, for example per location or business unit, and aggregates compliance status across projects.

### Article 83: General conditions for imposing administrative fines

Infringements shall be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

## GDPR Process Discovery Assessor

The GDPR Process Discovery application kick-starts your data gathering exercise through a simple set of questions, which can either be disseminated to functional heads via a questionnaire, or completed in a workshop environment, augmented by an expert GDPR facilitator. The questions are designed to capture key data inventory elements, such as business processes, information assets and systems. Based on the information entered, administrators benefit from risk-indicators, which can help focus follow-up deeper dive investigations. The output from GDPR Process Discovery can be pushed into the more granular Information Asset Management application.

### Article 30: Records of processing activities

Each controller shall maintain a record of processing activities that contains the name and contact details of the controller, the purposes of the processing, categories of data subjects and personal data, categories of recipients, transfers of personal data to third-parties, time limits for erasing data and security measures.


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**

# SureCloud GDPR Suite

## Information Asset Management

Information Asset Management underpins any regulatory or non-regulatory compliance framework. Information is captured in a granular and structured hierarchy, from top-level business processes, right down to the systems and infrastructure, which support them. A data inventory catalogs information held in each type of asset, and includes data subjects, data type sensitivity and internal data classification.

A centralized Data Transfers Register tracks how information flows both internally within the organization and externally to third parties. This information can be viewed using the Data Flow Visualization interactive tool and recorded data transfer can then be used to complete Records of Processing Activities requirements.

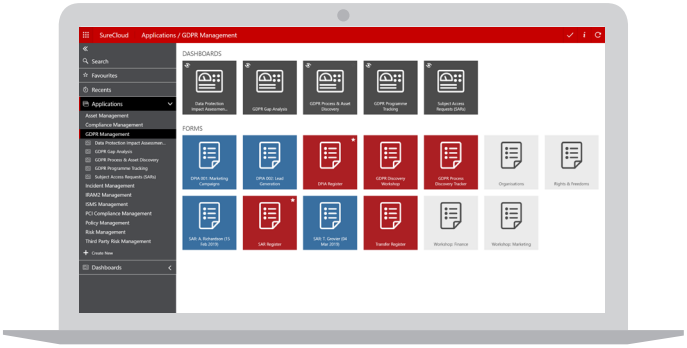
### Article 30: Records of processing activities

Each controller shall maintain a record of processing activities that contains the name and contact details of the controller, the purposes of the processing, categories of data subjects and personal data, categories of recipients, transfers of personal data to third-parties, time limits for erasing data and security measures.

## GDPR Management

GDPR Management provides mandatory business-as-usual processes:

1. Facilitation of Data Protection ImpactAssessments (DPIA) - screening questions that determine the need to address roles and responsibilities, principles, privacy risks and consultation with data subjects/supervisory authorities.
2. Collecting and managing subject requests within the 1-month period for all GDPR rights, such as erasure, data portability and restricted processing.



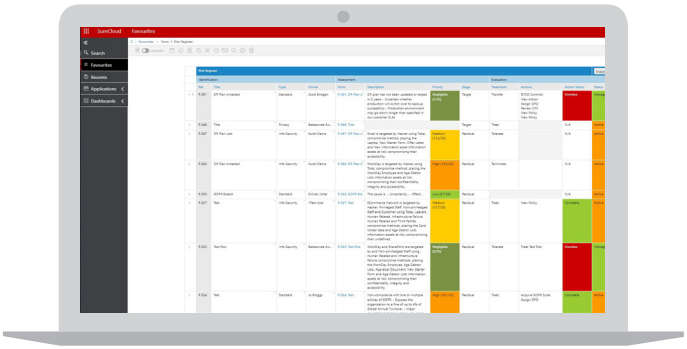


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**

# SureCloud GDPR Suite

## Risk Management

Risk Management allows you to identify the sources of risks to the rights and freedoms of individuals, such as employees and customers, as described in the EU GDPR and the European Convention on Human Rights (ECHR). Use this tool to build your organization-specific context for the privacy issues identified by multiple Data Protection Authorities (DPA) and the European Commission (EC).



### Article 35: Data Protection Impact Assessments

Prior to the processing, the controller shall seek the advice of the data protection officer and carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

## Compliance Management

Compliance Management addresses ongoing compliance requirements by providing a streamlined process for managing and reporting on GDPR controls, and demonstrating ongoing compliance. Use the status and maturity of controls to help reduce risks to residual and desired targets.

### Article 32: Security of Processing

The controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.

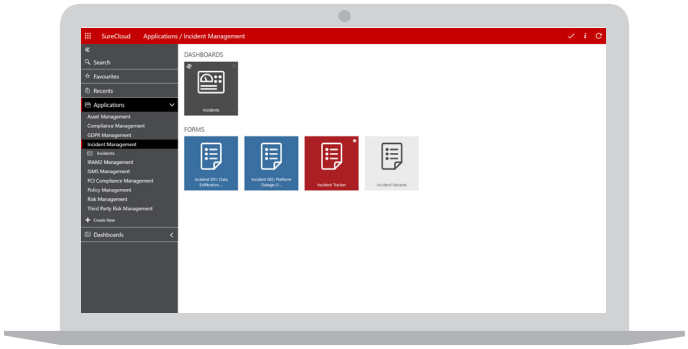

**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

# SureCloud GDPR Suite

## Incident Management

Incident Management meets the GDPR requirement to log, track and notify of data breaches. It tracks incident nature, categories, number of data subjects and personal data records concerned. Furthermore, it tracks planned investigation and mitigation work. And a built-in data breach notification report is automatically generated and populated from the incident log to speed notifying appropriate data protection authorities.




> **“ We chose Surecloud because of its recognised cybersecuirty, expertices, technology platform, speed in delivery and budget friendly pricing.**
>
> Alexander Tange, Co-founder and CEO, ICM Hub

## Article 33: Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall notify the supervisory authority within 72 hours.

## Trusted by Companies around the world:

JUST EAT · Dixons Carphone · Everton 1878 · TGI FRIDAYS · Thames Water · SHOP DIRECT

## Book your demo

**Make GDPR complexity a thing of the past. If you’re ready to turn GDPR compliance to your competitive advantage, it’s time to book your demo of SureCloud GDPR Suite.**

**Email: sales@surecloud.com**

**Start your GDPR project today.**


**US:** (+1) 310-318-4883 sales@surecloud.com
**UK:** +44 (0) 208 012 8544 **www.surecloud.com**


SureCloud®

SureCloud®

SureCloud is a provider of cloud-based, integrated Risk Management products and Cybersecurity services, which reinvent the way you manage risk. SureCloud is underpinned by a highly configurable technology platform, which is simple, intuitive and flexible. Unlike other GRC Platform providers, SureCloud is adaptable enough to fit your current business processes without forcing you to make concessions during implementation; meaning you get immediate and sustained value from the outset.

www.surecloud.com

Corporate Headquarters
SureCloud Limited.
10 Brick Street, Mayfair, London,
W1J 7DF UK +44 208-012-8544

SureCloud Inc.
6010 W Spring Creek Pkwy
Plano, TX 75024
United States of America

Phone: +1 (972) 996-6989

sales@surecloud.com