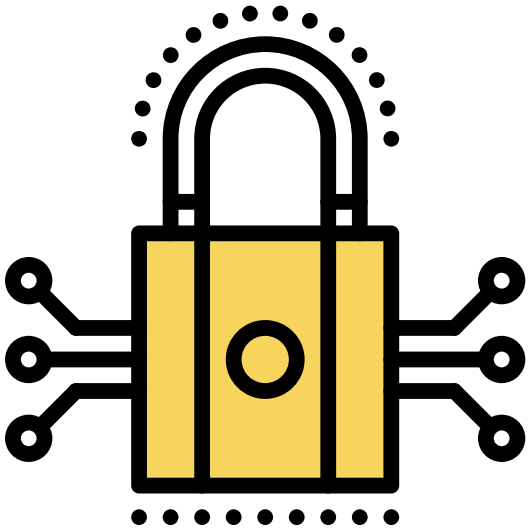
EVERYCLOUD
BE CLOUD CONFIDENT

IS YOUR CLOUD READY FOR GDPR?

Guide to the 6 most important GDPR articles for cloud compliance.

CONTENTS



EXECUTIVE SUMMARY

These are the 6 most important GDPR articles from the GDPR regulations which identify some of the biggest issues in becoming GDPR compliant.

- **ARTICLE 25:** Data protection by design and by default
- **ARTICLE 28:** Data Processors and Contractual Arrangements
- **ARTICLE 32:** Security of data processing
- **ARTICLE 33:** Notification of a personal data breach
- **ARTICLE 34:** Notifying breaches to data subjects
- **ARTICLE 35:** Data protection impact assessment

This guide will help you and your company understand exactly what each of the six key articles means for cloud applications and data storage and use, and how to best prepare for their enforcement.

GDPR will cause huge upheaval for any organisation gathering and processing personal data. But one of the biggest risks to normal operations is likely to come from the ever-expanding use of cloud applications.

Almost 30% of the data processed by businesses* is being used in unsanctioned cloud applications. This poses a huge compliance issue as GDPR places the onus on businesses to protect data. Simply relying on service providers to do it for you is no longer enough.

To avoid GDPR's hefty penalties, businesses must begin formulating a strategy for sensitive and personal information being stored in cloud services.

TO FULLY COMPLY, EVERYCLOUD RECOMMENDS A FOUR-STEP APPROACH

DISCOVER	Determine which personal identifiable data is being processed and stored in cloud applications
AWARE	Identify the cloud applications your people use – approved or otherwise
COMPLY	Prevent personal, sensitive and special data from being uploaded or processed to unmanaged or unsanctioned applications
CONFIDENCE	Protect data when uploading to cloud applications and prevent data leakage outside of your organisation

*According to www.computerweekly.com - "UK organisations lose £217m a year due to lack of cloud skills"

IS YOUR CLOUD READY FOR GDPR?

Whether or not you're one of the businesses who still haven't made preparations for GDPR, the new regulation will be in force from the 28th May 2018.

It will fundamentally transform the ways in which businesses can use customer, employee, and general population data to drive revenue, deliver services, and optimise their cost profiles.

It also creates a considerable new compliance burden for private and public bodies alike. In the age of the cloud, this represents a particular challenge, as data moves freely between different servers, devices, and networks.

Often, these are located in different countries or even on different continents – with very different data protection standards.

Moreover, the vast majority of the data accessed by businesses these days is unstructured. Unrestricted by any clear, company-wide policy. And over 30% of this data is being used in unsanctioned applications with unknown data protection approaches. And that has to stop.

From 28th May 2018 onwards, all businesses using cloud services will have to very seriously consider several specific things about how, where, and for whom these services operate.

The legislation itself is a lot to swallow. It spans 11 chapters and 99 articles. But we've highlighted **six key articles** you'll need to consider when formulating your new cloud security policy.

Most importantly, almost all cloud services currently have Terms of Service (TOS) provisions that do not conform to the requirements of GDPR. This is especially true when it comes to the storage, processing, and disposal of sensitive data. Businesses will be forced to completely re-evaluate their continued use of cloud applications in light of this, and act accordingly.

"The legislation itself is a lot to swallow. It spans 11 chapters and 99 articles."

ARTICLE 25: DATA PROTECTION BY DESIGN AND BY DEFAULT

The Terms

The data controller is responsible for ensuring that their organisation has put in place appropriate technical and policy safeguards to protect personal data.

Controllers are only expected to do what is reasonably scalable and cost effective in this aim – though 'appropriate' must take into account the current state of the art.

Personal data can only be stored or processed if it is earmarked for a specific use, within a specific, delineated time period. And this must be done in a way that ensures data cannot be attributed to an 'identified or identifiable' data subject.

The Implications

It will no longer be possible to indiscriminately warehouse data on any platform. Cloud services are no exception, and company policy must be created to prevent it.

Any cloud services your organisation uses will need to be vetted for GDPR compliance, and for the robustness of their own inbuilt security architecture.

You'll also be expected to provide an architecture and policy for your own ecosystem that meets with the rather broad requirements of the article – as advanced as possible without being unreasonably costly or impractical to run.

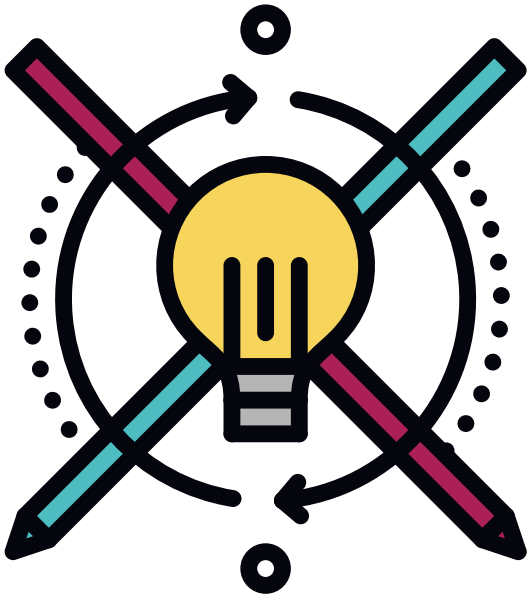
Your Actions

Create a clear, unambiguous set of rules around what your organisation will use data for, how long it will store it, and what measures it will take to protect it.

Determine which services are used in your organisation, sanctioned or otherwise, including those used privately by your staff.

Make sure you have the ability to deny access to unsanctioned applications as well as these that cannot meet the GDPR's protection by design criteria.

Ensure data is encrypted prior to upload to cloud servers. This will help satisfy the requirement that personal data will not be linked with their owners.



ARTICLE 28: DATA PROCESSORS & CONTRACTUAL ARRANGEMENTS

The Terms

If you can't process data yourself, you have to nominate a competent data processor to do the job for you. 'Competent' means they know how to follow the provisions of the regulations. They can't outsource the work to anyone who isn't able to do it to the same standards.

Any processing work 'passed on' like this has to be governed by a very specific contract called a 'data processing agreement'. It's a legally binding agreement that makes sure the processor agrees only to handle data for the specific reasons the controller collected it in the first place, and commits them to similar standards of confidentiality.

The processor must also follow the same rules regarding technical and organisational approaches to security. In the event of violations, processors and controllers share responsibility.

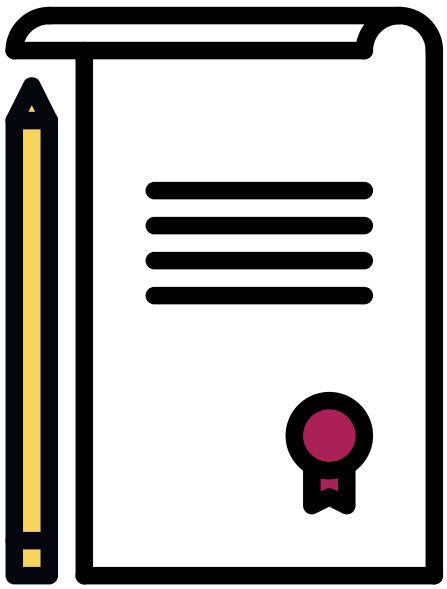
The Implications

Unless you're processing your data in-house, you'll probably have to revisit your agreements with the companies that do it for you. This will, of course, also apply to any outsourced analytics platforms you're using to store and sift personal information.

Since data processors are empowered (and expected) to let you know if any of your requests infringe on the act, you should expect a much closer relationship with them. Along with a stricter set of practices in that relationship.

Your Actions

1. Make a thorough assessment of who processes data for your organisation, and how they do it.
2. Pay particular attention to sanctioned and unsanctioned cloud applications.
3. Be ready to adopt stringent data processing agreements in line with Article 25 – specifying exactly what data is collected, processed, and stored, and how and by whom this is done.
4. Ensure contractual agreements are in place with all cloud providers or applications that process or store personal, sensitive information.



ARTICLE 32: SECURITY OF DATA PROCESSING

The Terms

The data controller and data processor must ensure that appropriate security measures are in place at all times during the processing of personal data. They must develop a specific and well delineated 'data processing agreement'.

This includes, but is not limited to, pseudonymising or encrypting personal data during processing, and maintaining 'confidentiality, integrity, availability, access, and resilience of processing systems and services'.

The controller and processor are also jointly responsible for restoring availability and access to personal data in the event of a breach, and for keeping security programmes and processes up to date. Adherence to an 'appropriate code of conduct' will be used to gauge this element of compliance.

The Implications

While Article 25 requires that you know which specific data you are recording/processing, Article 32 requires that you pay attention to how it's processed.

Unauthourised processing or alteration of data (i.e. any activity outside the processing agreement) constitutes a violation – except where law requires the data to be processed outside the agreement.

But beyond this, data loss – whether from a breach or negligence – also constitutes a violation.

All of these provisions are particularly important in the light of cloud services. Most cloud services do not currently have service terms that accommodate GDPR standards, making them unsuitable for use. Furthermore, data in cloud services can easily be lost or made unavailable in service outages, or moved from sanctioned to unsanctioned platforms unintentionally.

Your Actions

1. Determine your data processing agreement and ensure it's executed fully – without interference from unsanctioned applications or leftover BYOD initiatives.
2. Amend your data capture activities. Only collect personal data you intend to process. 'Special cases' no longer exist, and could land you with a considerable fine if they come to the attention of the authorities or the data's owner.
3. Ensure that all data is erased once service ends, or once the stated processing purpose is completed.
4. Establish who 'owns' the data present in your cloud applications and exactly who is likely to process it.

"While Article 25 requires that you know which specific data you are recording/processing, Article 32 requires that you pay attention to how it's processed"

ARTICLE 33: NOTIFICATION OF A PERSONAL DATA BREACH

The Terms

The data controller must notify their supervisory authority of a data breach within 72 hours where feasible, and provide adequate reason if they can't.

You'll be expected to describe the extent of the breach, the number of data subjects affected, the likely consequences of the breach, and proposed remedial actions – both to recover lost data, and mitigate any negative outcomes.

The Implications

Breaches will likely come to constitute an even more disruptive force on businesses and customer trust, as it will be difficult to manage optics and brand-based damage control tactics on such short timelines.

The requirement to describe the extent of the breach, the precise personal data affected, and the subjects in question will put companies in a very difficult position if – like many – they have been collecting data outside of official policies.* This is especially important for data stored in cloud services.

It will be obvious that you haven't been following the rules when you have to tell the supervisory authority that you don't know the full extent of the breach because of badly-managed cloud applications.

Your Actions

1. Skill up your teams to respond to breaches in double-quick time.
2. Determine the most likely source of breaches and vulnerabilities.
3. Make sure that your data processors and cloud partners have their own security watertight where possible – and be ready to cease using them if they don't.
4. Establish a clear cyber security response plan and train your team on how to communicate a breach.

> *"It will be obvious that you haven't been following the rules when you have to tell the supervisory authority that you don't know the full extent of the breach"*

*For this reason, most data collected prior to your adoption of a specific GDPR-informed data policy will most likely have to be discarded.

ARTICLE 34: NOTIFYING BREACHES TO DATA SUBJECTS

The Terms

When a breach poses significant risk to a data subject, they must be notified without delay. The notification must specify exactly what data has been lost, and the potential implications this might have. It must also detail the measures taken to retrieve data and mitigate ill-effects, as outlined in Article 33.

Breaches must only be reported if data was not properly handled/safeguarded or made unintelligible by technological means (e.g. through encryption). But your supervisory authority has the final say on whether or not you actually have to disclose a breach to subjects.

In cases where individual notifications would be impractical, public announcements must be made to address the extent of breaches and the following remedial actions.

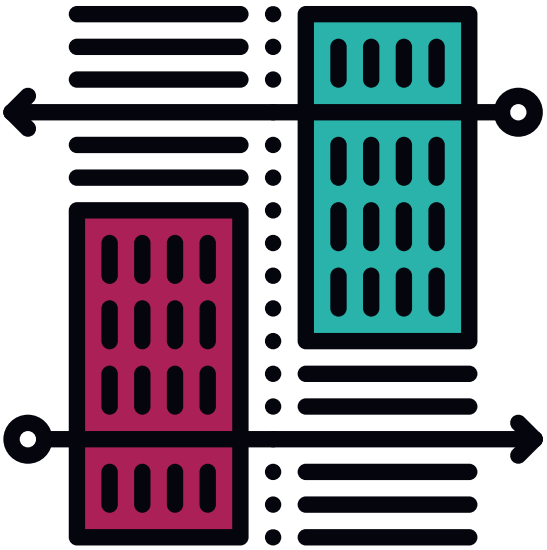
The Implications

Mistakes won't just cause direct damage to your company's reputation. They'll cause damage indirectly each time you have to inform a customer, employee, or other stakeholder that you have lost their data.

Most cloud services' ToS provisions are currently radically misaligned with the requirements of GDPR.

Your Actions

1. Skill up your teams to respond to breaches in double-quick time.
2. Determine the most likely source of breaches and vulnerabilities.
3. Make sure that your data processors and cloud partners have their own security watertight where possible, and be ready to cease using them if they don't.



ARTICLE 35: DATA PROTECTION IMPACT ASSESSMENT

The Terms

When processing data is likely to cause 'high risk to the rights and freedoms' of individuals, the controller must conduct a Data Protection Impact Assessment. This process is intended to show how likely it is that processing sensitive data will compromise its safety.

What exactly constitutes 'sensitive data' is not specified explicitly. However, advice given by supervising authorities indicates it will definitely extend to the following:

1. Data revealing an individual's financial or economic status.
2. Data that may lead to stigmatization or discrimination.
3. Credentials (e.g. usernames and passwords).
4. Data protected by legal/professional secrecy obligations.
5. Data that can be used to commit identity fraud.

Further to this, impact assessments must be conducted in any cases where data concerns a very large number of people, or the long-term monitoring of publicly accessible areas.

Assessments must be undertaken in consultation with your DPO. And they must detail the scope and content of processing, its purpose, its necessity, the nature of potential risks, and the special measures being taken by the processor and controller to mitigate those risks.

You may also be expected to consult the subjects of sensitive data for their views and concerns in these instances.

The Implications

With some exceptions, the compliance burden inherent in processing 'sensitive' data like this may make doing so impractical in most instances. This also applies to the much more rigidly defined 'special data' category, processing of which is usually forbidden.

More than any of the other 5 articles we've covered, Article 35 will have the most dramatic impact on how your company uses cloud services.

HOW EVERYCLOUD CAN HELP

EveryCloud provides independent consultancy on cloud security, and because we're truly independent, we tailor our solutions to the precise needs of your business, with a view to future growth.

We advise on all aspects of cloud security. Providing insight and recommendations on cloud access, identity management, and traditional email and web security services.

The cloud can be a dangerous place for your data and devices. Especially when you're not sure who's using what, where, or when.

Our Cloud Risk Assessment puts you on the path to a 360-degree view of your business's cloud presence across both your sanctioned and unsanctioned applications. In the process, we'll reveal threats to your data security, make sure you're compliant with industry regulations, and identify compromised accounts and malware infections.

We'll also give you a risk-resolution roadmap to overcome the biggest problems you face today – and a glimpse of your posture in the wider risk landscape.

"The explosive growth of cloud services is a major challenge in the enterprise space. Cloud services are here to stay; they are rapidly becoming the normal way to collaborate, communicate and interact with your friends, colleagues and clients."

FRASER DICKSON,
CYBER SECURITY MANAGER - BDO

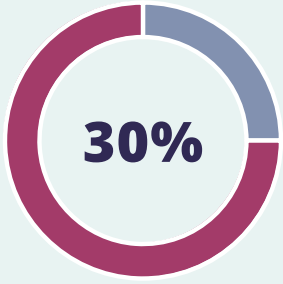
"Data security is a key priority for the club. Information on players and their contracts is a vital asset for us and fans also entrust us with their data, including personally identifiable information. We take this responsibility seriously so we're keen to provide employees with the right tools to boost productivity without compromising on security."

PHIL DAVIES,
ICT MANAGER - EVERTON FC

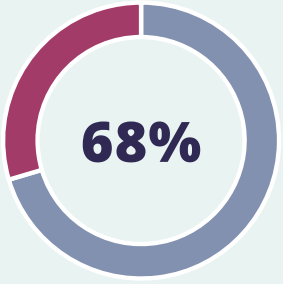
KEY FINDINGS FROM EXAMPLE CLOUD RISK ASSESSMENT

Number of cloud apps discovered – 40% higher than industry average

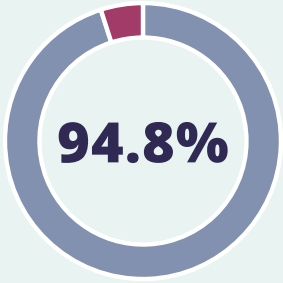
Apps with unclear data ownership



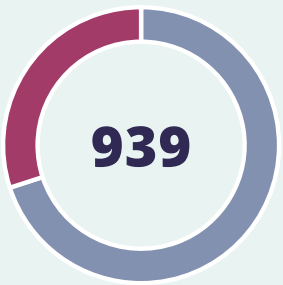
% of all data uploaded goes to unsanctioned cloud apps.



Percentage of apps violating GDPR



% apps non enterprise ready not meeting basic standards



Number of apps that cannot erase your data when you leave the service

RECOMMENDATIONS TO BUSINESSES

Determine what personal data your organisation currently processes or stores in cloud services.

Compliance starts with knowing the scope of your data processing. And while it's relatively easy to know what data is stored in on-premise enterprise systems, working out what's made its way to the cloud is much harder.

You'll need to undertake a full programme of 'data mapping' to discover the full extent of personal data in your cloud applications. That means you'll need a tool capable of doing it.

Identify the cloud applications your people are using.

As well as knowing what services are being used within the company, you'll need to know what their policies are on data collection, processing, and retention.

Some tools currently on the market will actually tell you which applications are and aren't GDPR compliant, making this process much more straightforward. If an application can't comply with GDPR, it can't be used by your company to store personal identifiable information.

You'll also need to know each application's policies on data migration, ownership and deletion as GDPR tightly controls the movement of data between legal jurisdictions, and many cloud services still use EU and non-EU servers indiscriminately as well as having questionable data ownership policies.

Prevent data being stored or processed on unmanaged/unsanctioned services.

As well as staff education, you will likely require some form of CASB (Cloud Applications Service Broker) to prevent or control your company's sensitive personal data being uploaded to unsanctioned cloud applications.

A CASB should be selected for the ability to specifically block data based on content and on format as things like pictures will often contain data-types such as racial origin which are outright prohibited under GDPR. It must also be able to distinguish between personal and corporate versions of the same application (i.e. Dropbox).

When data must be uploaded, ensure it's protected.

GDPR explicitly states that it's your responsibility to take steps to protect personal data. Meaning it's no longer sufficient to rely on your cloud applications' security to protect data.

The most obvious choice is to employ a tool which can encrypt all data before it's uploaded. Then, even if it is intercepted by malicious actors en-route to the cloud or while stored there, it will be unintelligible.

GLOSSARY OF TERMS

GDPR comes with a vocabulary of its own. So you're not completely in the dark, we've compiled a short list of definitions.

DATA CONTROLLER: The person or entity gathering and 'owning' personal data. In most instances of security, this will mean you and your business more generally.

DATA SUBJECT: The individual to whom personal data refers.

DATA PROCESSOR: An individual or company engaged by a data controller to process personal data on their behalf. Subject to a similar set of controls and obligations.

DATA PROCESSING AGREEMENT: The contract between a controller and processor, setting out the specifics of a processing task.

DATA PROTECTION OFFICER: An internal member of staff (which may be contracted out) responsible for assessing and ensuring any organisation's compliance with GDPR.

SUPERVISORY AUTHORITY: A regional or national authority set up by an EU member state to oversee GDPR compliance and the conduct of organisations and individuals.

PERSONAL DATA: Any data concerning an 'actual person'.

SENSITIVE DATA: A subset of personal data deemed to pose a potentially higher risk to a data subject. Its exact scope is not precisely defined.

SPECIAL DATA: A more closely defined subset of Sensitive Data. Includes data relating to personal beliefs, trade union membership, ethnicity and race, health (including sexuality), genetics/biometrics, and criminal convictions. 'Special Data' is considered to pose such a high risk to individual rights that processing it will almost always be prohibited.

EVERYCLOUD
BE CLOUD CONFIDENT

Heron Tower, 110 Bishopsgate
London - EC2N 4AY.
Email: discover@everycloud.co.uk.
Phone: 0800 470 1820.