GDPR In A Nutshell

The biggest change to our data protection laws in 20 years. Are you ready?

Deadline: 25th May 2018

“Three quarters of us don’t trust businesses to do the right thing with our emails, phone numbers, preferences and bank details. I find that shocking.”

Elizabeth Denham
UK Information Commissioner

Who Does GDPR Apply To?

On the 25th of May 2018 the EU's General Data Protection Legislation (GDPR) will come into effect. It will impact millions of businesses, of every size.

pwc

GDPR will apply to every entity that holds or uses European personal data both inside and outside of Europe.

Myths & Facts Leading To Complacency

The truth is GDPR likely applies to you.
You should start getting prepared now for May 2018.

48% of UK citizens are planning on using their new GDPR rights. **15%** in the first month. Get ready!

One in Three

Businesses haven't even heard about GDPR yet.

Serious Offenses

Up to €20m or 4% of turnover.

Lesser Offenses

Up to €10m or 2% of turnover.

More Awareness

ICO will be running an awareness campaign.

Brexit Effect

The UK leaving the EU does not effect GDPR.

Only Security

Having good data security is not enough.

Doesn't Apply

It applies to businesses of ALL sizes and types.

Current Data

It's not only future data, it's your current data too.

Have Time

There isn't much time left to become compliant.

GDPR And Fear-Mongering

It's true there are real consequences, and heavy penalties, for not complying with GDPR. However the new law is also an extremely positive development, and if anything, long overdue. Organisations should **seize this opportunity** to transform their company into a customer-centric, data-driven entity with the right internal controls and technology.

52%

of companies believe the cost of implementation was fully justified based on the benefits delivered.

98%

say the biggest benefit they saw was improved information security.

69%

say the main factor for choosing to adopt and implement was to improve organisational structure.

Source: gdprcoalition.ie

Opportunities & Consequences

The focus is usually on the negatives of non-compliance,
but there are a lot of positives businesses should take advantage of.

Non-Compliance

Fines Up To **4% Of Revenue**

Fines Up To **€20 million**

Class Action Lawsuits

Disruption To Business

Brand Damage

No Case Law

Compliance

Efficient Data Management

Streamlined Processes

Transparency

Security

Data Encryption

Better Internal Controls

Risk Reduction

Data Encryption

Less long-term cost

Updated Technology

“Isn’t having customers’ trust a cornerstone to good business? Isn’t that intangible relationship with customers: loyalty, trust, repeat customers, something most companies want?”

Elizabeth Denham
UK Information Commissioner

The Four Key Areas

This guide will be covering each, in our quest to transform you into a GDPR Guru!

PART 1

Your New Rights

What new rights do people now have?

PART 2

Consent & Privacy

How to get permission to use people's data?

PART 3

Personal Data

What is it, and how to manage it?

PART 4

Action Plan

What steps must you take to comply?

Note: we take no responsibility for the completeness or accuracy of this information.
Please do your own research, or seek consultation around your own specific obligations.

Remember, Good Software Is Key

Comply with GDPR, and all current and future laws more easily with the right software.
Here a just a few essential features you will need:

Auto-Filing & Archiving

Organise your data, store it easily & accurately in a compliant manner.

Manage Internal Processes

Workflows + tasks to streamline & document your business processes.

Centralise Your Data

Copy all data from network, local, USB, paper & Outlook to 1 place.

Right To Be Forgotten

Find all of a customer's records if you need to delete them.

Secure Customer Portal

Secure all external correspondence. Plus retract messages + more.

Audit Trails

Easily carry out reviews & report on data breaches within 72 hours.

Security & Encryption

2-step verification, end-to-end encryption & access permissions.

Document Retention

Set an expiry date on documents after which they are auto-deleted.

Principle Of Least Privilege

Minimise personally identifiable data managed by your teams.

Need To Know

Grant access on specific role or involvement, not hierarchy.

Privacy By Design

Software that lets privacy become a default part of your operation.

Staff Training

The tools & processes your staff need for ongoing compliance.

Tip: Virtual Cabinet's software does all of the above and more. Visit VirtualCabinet.com to book a Demo.

Before We Dive Into It

We know understanding your legal requirements can be difficult, proposed solutions often don't meet your intended needs, and every effort incurs significant time and disruption costs - **so please don't suffer it alone!**

Virtual Cabinet's software and specialists have helped 1,000's of businesses of every size become compliant with GDPR and other laws. Plus while you're at it, you'll get an instant return on your investment with better security, team workflows, collaboration, client communication, faster turnaround times, automated administration - and more.

So become compliant **and** get a more efficient business - in less time, and with fewer headaches. Win-win. Why not talk to one of our specialists today by clicking the link below:

Talk To A Specialist

Or visit VirtualCabinet.com

Mark
Available

Dave
Available

Murray
Available

United Kingdom Direct Contact
0845 166 1165
uk.hello@virtualcabinet.com

PART 1

Your New Rights

What new rights do
individuals now have?

Your New Rights: Overview

Powerful new super-powers to control your Personal Data

Right To be Informed

Individuals need to be informed when you collect or process their data.

Right Of Access

Individuals can now ask for access to their data, and why you are processing it.

Right To Rectification

Data that is inaccurate or incomplete must be corrected on request.

Right To Be Forgotten

Individuals can ask to have all their data deleted from your records.

Right To Restrict Processing

Individuals can 'block' any further processing of their data.

Right To Data Portability

Individuals can obtain and reuse their data on different services if they choose.

Right To Object

Individuals can object to data being processed in marketing, research etc.

Automation & Profiling Rights

Safeguards to protect individuals against automated decisions & profiling.

Tip: software can help you become GDPR compliant with the least effort.

VirtualCabinet.com does a good job of this. Visit their site to book a demo and see if they can help.

OK, But What Do ‘Rights’ Practically Mean?

Skip to Part 2 if you want to avoid specifics. Or keep reading for a meaty breakdown of what each ‘Right’ practically means for you.

Right To Be Forgotten

You must erase personal data on request, or when you have finished processing it.

Tip: Use software to **automatically** file incoming data into a centralised spot.

Finding and deleting an individual’s data then becomes much easier. VirtualCabinet.com does this well.

You Must Erase Data When

- When the data is no longer necessary for the original purpose it was collected for.
- When an individual withdraws their consent.
- When individual objects to processing.
- When the data was obtained unlawfully.
- When the law requests it.

When Can You Refuse To Erase

- When it obstructs your freedom of expression.
- When the law requests it.
- Public interest in the area of public health.
- Archiving purposes in the public interest.
- Exercise or defense of legal claims.

Children’s Personal Data

There are increased rights for children to request erasure.

Third Party Erasure

If data has been disclosed to any third parties, they must be informed about any data’s erasure, unless this involves disproportionate effort.

Right To Be Informed

Individuals need to be informed when you collect or process their data:

- In clear, plain, concise language
- Free of charge

If Collecting The Data Directly:

You must inform the individual of:

- Your Organisation's identity.
- Your Data Protection Officer's identity.
- The purpose of the data processing.
- The legal basis for your data processing.
- Details of transfer to any third country.
- The retention period, or criteria.
- The existence of the individual's rights.
- Their right to withdraw consent at any time.
- Their right to complain to a supervisory authority.
- Existence of any automated decision making, including profiling.
- If provision is part of a statutory or contractual requirement, and consequences of not providing data.

If Collecting The Data Indirectly

You must inform the individual:

- In a reasonable period (within 1 month).
- When communicating with the individual.
- When disclosing data to another party.

And as well as all the information (to the left) you must supply when collecting the data Directly, you must also inform the individual of:

- Categories of personal data.
- The original source of the data, and if it was publicly accessible.
- However, you do not need to explain whether the data provision is part of a statutory or contractual requirement.

Right Of Access

Individuals will be able to access:

- Confirmation their data is being processed
- Access to their personal data
- Other supplementary info

Tip: ensure you each document has an audit trail showing who has accessed it and why. VirtualCabinet.com does this automatically.

How Long Do You Have To Comply?

One month. Two months if requests are complex or numerous (but you must inform the individual).

Can You charge a fee?

No. It must be free unless the request is 'manifestly unfounded or excessive'.

What If The Request Is 'manifestly unfounded or excessive?'

In this case, particularly if the request is repetitive, you can either:

- Charge a fee based on administration costs.
- Refuse to respond, explaining to why & their right to complain to a supervisory authority.

How Should The Information Be Provided?

- You must verify the identify of the person making the request using 'reasonable means'.
- If the request is electronic, you should provide the information electronically.
- Where possible organisations should provide remote access to a self service system.

Requests For Large Amounts Of Personal Information?

You may ask the individual to specify the information the request relates to.

You can use this as part of your consideration as to whether the request is 'manifestly unfounded or excessive'.

A lot people feel they've lost control of their own data. People feel that keeping control of their most important information used to be simple, but that over the years, their sense of power over their personal data has slipped its moorings."

Elizabeth Denham
UK Information Commissioner

Right To Rectification

Individuals can have personal data rectified if it is inaccurate or incomplete, without delay.

When Can This Be Used?

If accurate or incomplete the data must be rectified, including informing third parties.

Right To Data Portability

Individuals can obtain & reuse their data for their own purposes across different services.

They can use this data to find a better deal, or understand their spending habits.

When Can This Be Used?

- You must provide the data in a structured, commonly used, machine readable form.
- You may need to transmit the data directly to another organisation if the individual requests it, if technically feasible.

The Rights Of Others

- If the data concerns more than one individual, you must consider the rights of the other individual.

Right To Restrict Processing

Individuals can 'block' you from processing their data.

When Can This Be Used?

Processing must stop if an individual:

- Contests the data's accuracy.
- Objects to processing.
- Opposes erasure and requests restriction when processing is unlawful.
- Needs the data to establish, exercise or defend a legal claim.

Communication

You must inform the individual if you unblock their data for processing.

Right To Object

Individuals can object to the processing of their data.

If The Data Is For Direct Marketing

If it is, you must stop processing as soon as you receive the objection, and deal with it free of charge.

If The Data Is For A Legal Task, An Organisations Legitimate Interests, Or Research Work

You must comply with a right to object unless:

- You can demonstrate compelling legitimate grounds.
- Processing is for the establishment, exercise or defense of legal claims.

Automation And Profiling Rights

A safeguard against the risk a damaging decision is taken without human intervention. E.g. an online credit application.

When Can This Be Used?

Individuals have the right not to be subject to a decision when:

- It is based on automated processing.
- It produces a legal effect.

When Can't This Be Used?

- When entering a contract.
- Authorised by law.
- With consent.
- With a child.
- On special categories of data unless you have explicit consent, or it is necessary for public interest.

What Do You Need To Do?

You need to make sure individuals can:

- Obtain human intervention.
- Express their point of view.
- Obtain an explanation, or challenge it.

Profiling & Automation

You must ensure safeguards are in place when processing data for profiling purposes:

- Fair and transparent.
- Meaningful information around logic.
- Appropriate statistical procedures.
- Minimise errors by employing measures.
- Secure personal data & prevent discrimination.

PART 2

Consent & Privacy

How to get permission
to use people's data?

Once you obtain consent to use someone's data, use a system like Virtual Cabinet to ensure you uphold their privacy and protect their Rights with the least possible effort.

Book Demo At VirtualCabinet.com

The 12 Steps To Correct Consent

Remember this list whenever you collect data.
You should be aiming for a clear, affirmative statement of consent.

1

When & How To Get Consent

- When any information is collected.
- Positive, Opt-In boxes are accepted.
- Consent by 'non-action' is prohibited.
  eg: Auto-Check Boxes, Opt-Out boxes.
- Language should be clear, plain & accessible.

2

Be Transparent

- The purpose of collection must be clear.
- State what the data is going to be used for.
- Inform who the data will be shared with.
- Disclose how long will you keep the data.

3

Data Minimisation

- Personal information can only be collected for specific, explicit and legitimate purposes.
- Only collect the minimum data you need.

4

Data Integrity

- Data must be confidentially and securely processed by your data system.
- Only authorised individuals should have access to the data consented to.

5

Data Time Limit

- All data must have an expiry date.
- The expiry date must be appropriate for the collected purpose.
- If unsure, it is recommended consent be checked every 2 years.
- Data cannot be stored indefinitely.

6

Data Accuracy

- You must ensure data is accurate and correct
- This is to avoid distress or harm to the individual.

12 Steps To Correct Consent Continued...

7

Genuine Choice

- Individuals must be given a genuine choice.
- Service cannot be conditional on consent.
- Individuals be able to refuse, or withdraw consent without detriment.

8

Identify Yourself

- Provide your identity and contact information.
- Disclose your Data Protection Officer's details, if relevant.

9

Children

- Individuals under 16 cannot give consent.
- The UK May lower its age of consent to 13.
- Parental consent is required for anything other than counseling and preventative services.

10

Allow User Action

- Explain how to withdraw consent.
- Withdrawing consent must be as easy as giving consent.
- The Right to object to direct marketing must be clear.
- Special data categories (race, health, genetic) require explicit consent.

11

Uphold Individual Rights

- Must be able to change inaccurate data.
- Must know what date has been collected and how it will be used.
- Must be able to transfer the data to another system.
- Must be able to withdraw consent.

12

Documentation & Process

- Prepare a clear record of your consent policy.
- Review and check it continuously.
- Make sure your existing data has the correct consent.

"The new legislation creates an onus on companies to understand the risks that they create for others, and to mitigate those risks."

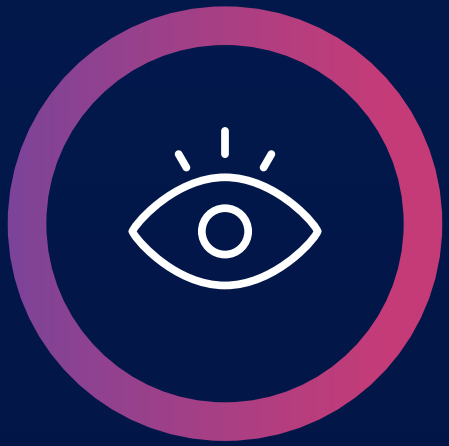
Elizabeth Denham
UK Information Commissioner

Privacy By Design

GDPR wants you to think about privacy and data protection
from the beginning, not as a bolted-on after-thought. This is 'Privacy By Design':

Limit Data
Only collect what is necessary.

Limit Processing
Only process data for the purpose that it was collected for.



Impact Assessment
Conduct assessments for personal data that is high risk to individuals.

Limit Access
Only authorised individuals should be able to access data.

Keep Reviewing
Keep checking the confidentiality, availability & resilience of your systems.

Record Keeping
Note processing, data categories, erasure time & storage locations.

PART 3

Personal Data

What is it, and how
to manage it?

Virtual Cabinet automatically files your data in one central spot so you have better Visibility, Control and Security over your business.

Book Demo At VirtualCabinet.com

What Is Personal Data?

‘Personal Data’ now includes any information relating to an identified natural person.
This could include a broad range of data including:

Name

Number

Location

Online ID

Physical

Physiological

Genetic

Mental

Economic

Cultural

Social

ACTION

Understand Your Data

What personal data do you hold? Where did it come from? Who is it shared with? Where do you keep it?

Consider an information audit to fully document & appreciate your data.

ACTION

Special Categories

Certain categories of data require particular care:

Race, Ethnic Origin, Politics, Religion, Trade Union Membership, Genetics, Biometrics, Health, Sex Life, Sexual Orientation.

Personal Data: Principles

Sticking to some simple principles will help you
master your Personal Data collection, transfer and storage

Stay Ethical

- Process data lawfully, fairly, transparently.
- Properly inform individuals if you collect it.

Specific Purpose

- Minimize the data you are gathering
- Only collect for defined a purpose.

Accurate

- Keep all your data up to date.
- Audit data for errors continuously.

Storage

- Only store data for as long as necessary.
- Ensure you have backups.

Security

- Restrict access to authorised individuals.
- Protect against loss and destruction.

Visibility

- Remember individuals can request their data anytime, so know where it is located.

Mandatory Data Protection Officer (DPO)

It is **mandatory** to appoint a DPO if you process or store large amounts of personal data.
One study predicts up to 28,000 DPO's will have to be hired by May 2018!

Power & Position

- Must operate independently, not taking instructions from their employer.
- Cannot be dismissed for performing their duties.
- Must be given sufficient resources.
- Must report directly to the highest management level in your company.
- Can be an existing employee. Or you can hire externally (including sharing the cost with other companies).

Responsibilities

- Train employees on GDPR compliance.
- Undertake audits, and solve data issues.
- Is your point of contact with the GDPR Supervisory Authority bodies.
- Maintain all evidence and reporting.
- Inform individuals how their data is being used, and how their rights are being upheld.

Qualifications

- There are no specific technical qualifications asked for by the legislation.
- The DPO must instead have 'expert knowledge of data protection law and practices'.
- Their expertise should be appropriate to your own company's data processing operations.
- The DPO's information must be publicly shared with all regulatory agencies.

Source: digitalguardian.com

Understand Your Data's Journey

From collection to destruction you should understand your Data's journey

Be Mindful Of Your Equipment

Review Equipment

- What equipment is at the end of its life?
- Eg. Computer Drives, Phones, Tablets, USD's and Security Badges.

Review Risk

- Make sure you have a disposal policy.

Cloud Storage

It is your responsibility to ask any online storage providers you use what their end of equipment life policy is.

Destroy It

- Devices must be physically shred to meet EU standards.
- Can be shred internally (with equipment), or destruction can be outsourced.

Transfer Data Correctly

Protection By Design

- Should be fundamental to all systems.

Impact Assessments

- Conduct when a transfer is high risk.

Data Security

- During all stages of data transfer and rest.

Safeguards

- Encrypt your data, use pseudonymisation.

Stick To Good Principles

- For example, only collect data you need.

Data Retention

- Maintain data retention schedules.

Reporting

- Document your process by collecting evidence.

PART 4

Action Plan

What steps must you take to comply.

7-Step Checklist To Compliance

STEP 1 Raise Awareness

- [ ] Make sure key decision makers know what is happening with GDPR (share this guide with them!)
- [ ] Staff training: most breaches occur through staff ignorance.
- [ ] Get strong commitment from the board & C Level Officers to build compliance culture.

STEP 2 Form A Team

- [ ] Form a cross functional data team including the IT team & business leadership.
- [ ] Appoint a Data Protection Officer (DPO) if needed.
- [ ] Team should be responsible for GDPR.
- [ ] Team should own the documentation process.
- [ ] Team should regularly review policies, processes and technology.

STEP 3 Do An Audit

- [ ] Start with an information audit & risk assessment of your data.
- [ ] Audit risk of servers, storage, end-point devices & cloud locations.
- [ ] Ensure you have a legal basis for carrying out data processing.
- [ ] Make sure you have consent for all your Personal Data.
- [ ] Review existing policies.
- [ ] Conduct a data-flow analysis to see how data moves & is stored.

7-Step Checklist To Compliance

STEP 4 Create A Plan

- [ ] Be proactive, don't think GDPR won't affect you – it will.
- [ ] Create a list of recommendations.
- [ ] Prioritise recommendations and assign resources and budget.
- [ ] Put together a roadmap to achieve compliance.
- [ ] Review your plan regularly.

STEP 5 Technology

- [ ] Move towards a single platform to organise all of your data.
- [ ] Get a single source of truth to better respond to data access, portability, erasure requests, data breaches, etc.
- [ ] Use technology from best vendor to stay ahead of the technology curve
- [ ] Try VirtualCabinet.com as a good software and systems solution.

STEP 6 Communication

- [ ] Put together an incident response process.
- [ ] Ensure you have a strong governance process.
- [ ] Plan how you will handling data requests within 30 days at no cost to individuals.

STEP 7 Individuals rights

- [ ] Be aware of the new Rights given to individuals under GDPR, as detailed in Part 1 of this guide.

"Last year we issued more than one million pounds in fines for breaches of the Data Protection Act, so it's not a power we're afraid to use."

Elizabeth Denham
UK Information Commissioner

Top Questions To Ask Your Departments

Legal

What's your plan for personal data requests? Is your process documented? Can it be automated? Can it scale? Response timescale? Published data retention policies?

Finance

Have you reviewed your processes to make sure they are managed securely? Potential penalties? Have you done risk planning?

IT

Which systems hold Personal Data? Could you find all data relating to an individual and delete it? Is it stored securely (office + cloud)? Any potential security breaches? Process for breach notification within 72 hours?

Marketing

When you capture consent for the use of Personal Data, do you explain why you need to have it and how it will be processed? Consent needs to be explicit. Individuals giving consent need to be fully informed.

HR

What personal data do you collect? Have you documented why it is captured? Do you obtain consent & explain how it will be processed? Have policies, forms & training been updated with new Personal Data categories?

Procurement

If a sub-contractor processes data on your behalf are their sufficient guarantees (especially expert knowledge, reliability & resources) to meet GDPR requirements?

Source: gdprcoalition.ie

Software Features You'll Need

Make sure the software you're using to become GDPR compliant has at least the following:

Auto-Filing & Archiving

Organise your data, store it easily & accurately in a compliant manner.

Manage Internal Processes

Workflows + tasks to streamline & document your business processes.

Centralise Your Data

Copy all data from network, local, USB, paper & Outlook to 1 place.

Right To Be Forgotten

Find all of a customer's records if you need to delete them.

Secure Customer Portal

Secure all external correspondence. Plus retract messages + more.

Audit Trails

Easily carry out reviews & report on data breaches within 72 hours.

Security & Encryption

2-step verification, end-to-end encryption & access permissions.

Document Retention

Set an expiry date on documents after which they are auto-deleted.

Principle Of Least Privilege

Minimise personally identifiable data managed by your teams.

Need To Know

Grant access on specific role or involvement, not hierarchy.

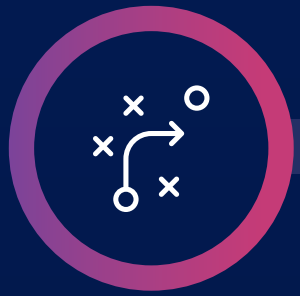
Privacy By Design

Software that lets privacy become a default part of your operation.

Staff Training

The tools & processes your staff need for ongoing compliance.

Tip: Virtual Cabinet's software does all of the above and more. Visit VirtualCabinet.com to book a Demo.



Where Do I Start?

The easiest way to become GDPR compliant is with the right software.

No matter your company size, book in a demo with a leading GDPR software provider like Virtual Cabinet to see if they can make your life easier.

Click To Book Demo

or visit VirtualCabinet.com

Still Confused?

We know understanding your legal requirements can be difficult, proposed solutions often don't meet your intended needs, and every effort incurs significant time and disruption costs - **so please don't suffer it alone!**

Virtual Cabinet's software and specialists have helped 1,000's of businesses of every size become compliant with GDPR and other laws. Plus while you're at it, you'll get an instant return on your investment with better security, team workflows, collaboration, client communication, faster turnaround times, automated administration - and more.

Become compliant **and** get a more efficient business - in less time, and with fewer headaches. Win-win. Why not talk to one of our specialists today by clicking the link below:

Talk To A Specialist

Or visit VirtualCabinet.com

Mark
Available

Dave
Available

Murray
Available

United Kingdom Direct Contact
0845 166 1165
uk.hello@virtualcabinet.com