GSDC

GLOBAL SKILL DEVELOPMENT COUNCIL

PLAIN-ENGLISH HANDBOOK

What is GDPR?

…and what does a DPO do?

A free, jargon-free handbook with every core concept in one reference: what GDPR is, what a Data Protection Officer actually does, DPIAs, breach rules and international transfers — plus an Article 37 explainer, a GDPR-vs-CCPA cheat sheet, and a starter DPIA guide. No legal background needed.

28-Page Field Guide • No Jargon • GDPR vs CCPA • DPIA Guide

One reference for the essentials

Data protection sounds complicated, but the core ideas are surprisingly approachable. This handbook explains them in plain English, in a sensible order, so you can read it cover to cover or dip in for a single concept. No prior legal or IT knowledge assumed.

WHAT IS GDPR? (IN ONE LINE)

The EU's data-protection law: rules that say organisations must handle people's personal data lawfully, fairly and securely.

WHAT DOES A DPO DO? (IN ONE LINE)

A Data Protection Officer advises on those rules, checks the organisation follows them, and is the point of contact for regulators.

SECTION 1

What is GDPR?

The plain-English version

GDPR stands for the **General Data Protection Regulation**. It's a law that came into force across the European Union in 2018, setting rules for how organisations collect, use and protect people's personal data. Its goal is simple: give individuals control over their own data, and hold organisations accountable for looking after it.

Why it reaches far beyond Europe: GDPR applies to any organisation, anywhere in the world, that handles the personal data of people in the EU. So a company in the US, India or Brazil serving EU customers must follow it too — which is why GDPR became the global reference point for privacy law.

What it protects

The personal data of individuals — their right to know what's collected, why, and to have a say in it.

Who it applies to

Any organisation that processes the personal data of people in the EU, regardless of where the organisation is based.

The big shift GDPR introduced: data protection stopped being optional good manners and became a legal duty — with real penalties for getting it wrong.

Personal data, explained

GDPR is all about "personal data," so it helps to know exactly what that means. **Personal data is any information that relates to an identified or identifiable person.** If it can be linked back to a specific human, it counts.

EVERYDAY PERSONAL DATA

- Name & address
- Email & phone
- ID & account numbers
- Location & IP address

"SPECIAL CATEGORY" DATA (EXTRA-PROTECTED)

- Health & biometrics
- Race & ethnicity
- Religious beliefs
- Sexual orientation

Special-category data is treated as more sensitive and carries stricter rules, because misuse could seriously harm someone. A DPO pays particular attention to it.

> **Quick test:** "Could this information, alone or combined with other data, point to one specific person?" If yes, it's personal data and GDPR applies.

The 7 principles of GDPR

At its heart, GDPR is built on seven principles — the rules of thumb every use of personal data must follow. In plain English:

1. **Lawfulness, fairness & transparency**
   Have a valid reason, be fair, and be open about it
2. **Purpose limitation**
   Only use data for the specific purpose you collected it for
3. **Data minimisation**
   Collect only what you actually need — no more
4. **Accuracy**
   Keep data correct and up to date
5. **Storage limitation**
   Don't keep data longer than you need it
6. **Integrity & confidentiality**
   Keep it secure — protected from loss or misuse
7. **Accountability**
   Be able to *prove* you follow all of the above

The one that changed everything: accountability. It's not enough to comply — you must be able to *demonstrate* it with records. That single principle is a big reason the DPO role exists.

The 6 lawful bases for processing

Before using personal data, an organisation needs a valid legal reason — a “lawful basis.” There are exactly six, and at least one must apply.

Lawful basis	In plain English — use it when…
Consent	The person has clearly agreed (opt-in)
Contract	You need it to deliver a contract with them
Legal obligation	A law requires you to process it
Vital interests	It’s needed to protect someone’s life
Public task	You’re performing an official public function
Legitimate interests	You have a genuine need that doesn’t override their rights

A common misconception: consent isn’t always required — it’s just one of six bases. Often “contract” or “legitimate interests” is the right and simpler choice. Picking the correct basis is a core DPO skill.

The rights of the individual

GDPR gives people — “data subjects” — a set of rights over their own data. Much of a DPO’s job is making sure the organisation can honour them.

1. **To be informed**
   Know what’s collected and why
2. **Of access**
   Get a copy of their data (a “DSAR”)
3. **To rectification**
   Have wrong data corrected
4. **To erasure**
   Be “forgotten” in certain cases
5. **To restrict & object**
   Limit or object to certain processing
6. **To portability**
   Take their data elsewhere in a usable format

The clock matters: organisations generally must respond to a rights request within **one month**. Knowing how to handle that request properly is everyday DPO work.

Controllers vs processors

Two roles GDPR keeps separate — because they carry different responsibilities. The difference is about *who decides*.

CONTROLLER

Decides *why* and *how* personal data is used. Carries the main legal responsibility. (e.g. a shop deciding to email its customers.)

PROCESSOR

Processes data *on the controller's behalf*, following instructions. (e.g. the email platform the shop uses to send those emails.)

An organisation can be a controller for some data and a processor for other data. Knowing which hat you're wearing decides which duties apply — so it's one of the first things a DPO works out.

> **A simple analogy:** the controller is the author who decides what a letter says; the processor is the courier who delivers it under instruction. Both handle the letter; only one decides its contents.

SECTION 2

What Does a DPO Do?

The role in plain English

A Data Protection Officer (DPO) is the person who makes sure an organisation handles personal data properly. Think of them as part adviser, part watchdog, part translator — turning complex law into practical action, and acting as the bridge between the organisation, individuals and regulators.

Adviser

Guides the organisation on its data-protection obligations and how to meet them.

Monitor

Checks that policies are followed and the rules are actually being met.

Point of contact

Liaises with the regulator and with individuals who have questions or complaints.

Risk-spotter

Advises on impact assessments and flags privacy risks before they bite.

A day in the life: reviewing a new project for privacy risk, answering a data access request, updating the records of processing, training staff, and being on hand when a potential breach is reported. Variety is the norm.

DPO responsibilities & the key Articles

The DPO role is defined in GDPR Articles 37–39. Here's what each one says, without the legalese.

37 **Designation**
When and how an organisation must appoint a DPO

38 **Position**
The DPO must be independent, properly resourced, and report to the top

39 **Tasks**
Inform & advise, monitor compliance, advise on DPIAs, cooperate with the regulator

Article 39 — the DPO's core tasks, in full

- Inform & advise the organisation & staff
- Monitor compliance with GDPR
- Advise on Data Protection Impact Assessments
- Cooperate with the supervisory authority
- Act as contact point for the regulator
- Consider risk in all of the above

These tasks are the backbone of the job — and a big part of what the certification prepares you to do.

When is a DPO required? (Article 37)

Not every organisation must appoint a DPO — but many must. Under Article 37, a DPO is mandatory in three situations.

1. **Public authorities**
   Any public body processing personal data (courts acting judicially aside)
2. **Large-scale monitoring**
   Core activities require regular, systematic monitoring of people at scale
3. **Large-scale special data**
   Core activities involve large-scale special-category or criminal data

INDEPENDENCE IS REQUIRED

A DPO must act independently, can't be told *how* to do the job, and reports to the highest level of management.

NO CONFLICT OF INTEREST

The DPO can't also be the person who decides the purposes of processing (e.g. not the head of marketing or IT).

Even when not strictly required, many organisations appoint one voluntarily — demand keeps growing.

SECTION 3

A Starter DPIA Guide

Data Protection Impact Assessments, simply

A **Data Protection Impact Assessment (DPIA)** is a structured way to identify and reduce the privacy risks of a project *before* it goes live. Think of it as a risk assessment, but for people's data.

When you need a DPIA

- Large-scale processing of sensitive data
- Systematic monitoring of public areas
- Profiling with significant effects on people
- New technologies that are high-risk

If a project is likely to result in a high risk to people's rights and freedoms, a DPIA isn't optional — it's required. When in doubt, doing one is good practice anyway.

Why DPIAs matter to a DPO: advising on them is one of the DPO's Article 39 tasks. Being able to run a solid DPIA is one of the most valuable practical skills in the role.

The DPIA, step by step

A DPIA follows a clear sequence. Here are the steps a starter assessment works through.

1. **Describe the processing**
   What data, why, how, how much, and for how long
2. **Assess necessity**
   Is the processing necessary and proportionate to the aim?
3. **Identify the risks**
   What could go wrong for individuals, and how badly?
4. **Plan mitigations**
   What measures reduce each risk to an acceptable level?
5. **Record & sign off**
   Document the outcome; consult the DPO; if high risk remains, consult the regulator

> **The mindset:** a DPIA isn't box-ticking — it's thinking through "how could this hurt someone, and how do we prevent it?" *before* building, when fixes are cheap and easy.

Breach rules — the 72-hour clock

A “personal data breach” is any security incident that leads to personal data being lost, stolen, exposed or destroyed. GDPR sets out clearly what must happen next.

TELL THE REGULATOR (ARTICLE 33)

Notify the supervisory authority within **72 hours** of becoming aware — unless the breach is unlikely to risk people’s rights.

TELL THE PEOPLE (ARTICLE 34)

If the breach is likely to be a **high risk** to individuals, tell them too, without undue delay, so they can protect themselves.

A simple breach response sequence

1. Contain & assess the breach
2. Judge the risk to individuals
3. Notify the authority within 72h (if needed)
4. Notify individuals (if high risk)
5. Record everything & learn from it
6. Improve controls to prevent a repeat

The 72-hour rule is one of the most-tested, most-quoted facts in all of GDPR.

International transfers, explained

GDPR protects data even when it leaves the EU. So sending personal data to another country — a “transfer” — comes with rules to keep the protection travelling with it.

1 **Adequacy decision**
The EU has ruled the destination country’s protection is strong enough — transfer freely

2 **Appropriate safeguards**
Use approved tools like Standard Contractual Clauses (SCCs) or Binding Corporate Rules

3 **Specific exceptions**
Limited situations (e.g. explicit consent, contract necessity) allow a one-off transfer

The core idea: you can’t escape GDPR simply by moving data abroad. The protection must follow the data wherever it goes — and a DPO makes sure the right mechanism is in place before any transfer happens.

This is one of the trickier areas of privacy, and it changes as laws and court rulings evolve — which is exactly why organisations value people who understand it.

Accountability & records

Remember the seventh principle — accountability? In practice it means keeping records that *prove* compliance. The central one is the Record of Processing Activities.

ROPA (Article 30)

A register of what personal data you process, why, who you share it with, and how long you keep it. The backbone of accountability.

Policies & notices

Privacy notices, data-protection policies and procedures that show how the rules are applied day to day.

DPIA records

Documented impact assessments for higher-risk processing.

Breach log

A record of incidents and how they were handled — even ones not reported.

Why it's a DPO's bread and butter: if a regulator ever asks "show me," these records are the answer. Keeping them current is one of the most important — and most practical — parts of the job.

Privacy by design & by default

Two phrases you'll hear often — and they capture a simple, powerful idea: build data protection *in from the start*, rather than bolting it on later.

PRIVACY BY DESIGN

Consider data protection at the design stage of every system or project — not as an afterthought once it's built.

PRIVACY BY DEFAULT

The most privacy-friendly settings should be the default — people shouldn't have to opt in to basic protection.

In practice this means asking, early: do we really need this data? Can we collect less? Who can see it? How long do we keep it? Answering those at the start prevents problems — and big costs — later.

> **The cheapest fix is an early one:** designing privacy in from day one is far easier than retrofitting it after a system — or a regulator — finds the gap.

SECTION 4

GDPR vs CCPA

A side-by-side cheat sheet

The CCPA (California Consumer Privacy Act, strengthened by the CPRA) is the best-known US privacy law. It shares GDPR's spirit but differs in key ways.

	GDPR	CCPA / CPRA
Who it protects	People in the EU/EEA	California residents
Applies to	Any org handling EU data	Businesses meeting CA thresholds
Consent model	Opt-in (basis needed first)	Opt-out (of data "sale")
Lawful basis	Required to process	Not required
DPO required?	In many cases (Art 37)	Not mandated
Max penalty	€20M or 4% global turnover	Per-violation fines + breach suits

Both aim to protect personal data — GDPR leads with "get permission first," CCPA with "let people opt out."

Beyond GDPR & CCPA

Privacy law is spreading fast. A modern DPO keeps an eye on the wider landscape, because so many of these laws echo GDPR's structure.

Law	Where	In brief
GDPR	EU / EEA	The global benchmark
UK GDPR	United Kingdom	GDPR retained post-Brexit
CCPA / CPRA	California, US	Opt-out consumer rights
LGPD	Brazil	Closely modelled on GDPR
PIPEDA	Canada	Consent-based federal law
DPDP Act	India	India's 2023 data-protection law

The good news for learners: master GDPR and you've learned the model most other laws follow. The concepts transfer — which is what makes privacy expertise so portable across countries and employers.

Penalties & enforcement

GDPR has teeth — which is precisely why organisations invest in getting it right, and why DPOs are in demand.

€20M
or 4% of global turnover — max fine

2 tiers
of penalty severity

Trust
reputational cost beyond fines

Fines come in two tiers: lower-level breaches (e.g. poor records) can reach €10M or 2% of turnover; serious breaches (e.g. violating people's rights) can reach €20M or 4% — whichever is higher. Regulators can also order an organisation to stop processing entirely.

> **Beyond the fine:** the reputational damage of a public breach — lost customer trust, headlines, churn — often costs more than the penalty itself. Prevention is the whole point of the DPO role.

The documents a DPO works with

To bring all of this together, here are the practical artifacts a DPO creates and maintains — the toolkit of the role.

- **Records of Processing (ROPA)**
  The Article 30 accountability register
- **DPIA templates**
  For assessing higher-risk processing
- **Privacy notices**
  Telling people how their data is used
- **Data protection policy**
  The organisation's rules, written down
- **Breach response plan**
  The 72-hour playbook
- **DSAR procedure**
  How to handle data access requests

This is the job, made concrete. A certification programme teaches you to build each of these — so you finish able to walk into the role, not just describe it.

Common GDPR questions, answered

A few everyday situations, to make the concepts concrete.

A customer asks for all the data we hold on them. What now?

That's a Data Subject Access Request. You generally have one month to provide a copy of their personal data, usually free of charge.

We lost a laptop with customer records. Is that a breach?

Potentially yes — assess the risk. If it's likely to risk people's rights, notify the regulator within 72 hours; if high risk, tell the individuals too.

Do we always need consent to use personal data?

No — consent is just one of six lawful bases. Often "contract" or "legitimate interests" fits better.

We're a US company. Does GDPR even apply to us?

If you handle the personal data of people in the EU, yes — GDPR applies regardless of where your company is based.

GDPR myths, busted

A few misconceptions trip up beginners. Let's clear them up.

MYTH	REALITY
"GDPR is only an EU problem."	It applies to anyone handling EU data
"You always need consent."	Consent is one of six bases
"GDPR bans keeping data."	You can keep data — just not forever, and for a reason
"Small companies are exempt."	Size doesn't exempt you; the activity matters

The theme: GDPR is less about banning things and more about doing them *responsibly and on purpose* — with a reason, a limit, and a record. Once that clicks, the whole law makes more sense.

Glossary of key terms

Every term in this handbook, defined simply.

GDPR — the EU General Data Protection Regulation; the benchmark privacy law.

Personal data — any information relating to an identifiable person.

Special category data — sensitive data (health, beliefs, etc.) with extra protection.

Data subject — the individual the data is about.

Controller — decides why & how data is processed.

Processor — processes data on the controller's behalf.

Lawful basis — the legal reason for processing (one of six).

DPO — Data Protection Officer; advises on and monitors compliance.

DPIA — an impact assessment of privacy risk before a project.

ROPA — Records of Processing Activities (Article 30).

DSAR — Data Subject Access Request.

CCPA / CPRA — California's consumer privacy laws.

Frequently asked questions

Do I need a legal background to understand GDPR?

No. As this handbook shows, the core ideas are approachable in plain English. A certification then builds depth and practical skill.

Is GDPR knowledge useful outside Europe?

Very — it's the model most modern privacy laws follow, so the concepts transfer worldwide.

What's the difference between a DPO and a privacy analyst?

A DPO is a defined, often legally required role with independence and specific tasks; analyst roles support the wider privacy programme.

How do I turn this knowledge into a career?

Build on these foundations with a recognised certification, then apply for privacy and data-protection roles — demand is strong and growing.

Where does the GSDC certification fit?

It takes the concepts in this handbook and develops them into job-ready, certified expertise — see the next page.

The one-page cheat sheet

The whole handbook, distilled to what's worth knowing cold.

6 LAWFUL BASES

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

KEY RIGHTS

- Be informed & access
- Rectification
- Erasure
- Restrict & object
- Portability

Numbers & articles to remember

· **72 hours** — breach notification

· **7 principles** — incl. accountability

· **€20M / 4%** — max fine

· **1 month** — respond to a DSAR

· **Art 37–39** — the DPO role

· **Art 30** — records (ROPA)

Keep this page handy — it covers the most-referenced facts in everyday privacy work.

Where the certification fits

This handbook gave you the *understanding*. The GSDC Data Protection Officer certification gives you the *proof* — and the depth — that turns interest into a career.

Think of it as the next step: this is “GDPR & the DPO, explained.” The certification is “GDPR & the DPO, mastered and certified” — built on the very concepts you’ve just read.

What it builds on

Everything here — principles, rights, the DPO role, DPIAs, breaches, transfers — taught in depth with practical exercises.

Who it’s for

Beginners and career-changers included — based on Privacy, Security & Governance principles, studied at your own pace.

$131K
avg. US DPO salary*

Global
recognised credential

Growing
demand for DPOs

*Glassdoor, US market; varies by experience, role and location.

GSDC

Now you know what GDPR is — and what a DPO does.

GDPR and personal data explained, the DPO role and Article 37, a starter DPIA guide, a GDPR-vs-CCPA cheat sheet, plus breach rules and transfers — the essentials, in one plain-English reference. You came in with a question; now you have the answers.

Next steps & resources

Explore the frameworks
Go deeper into the standards & the role.

Discover the DPO program
The beginner-friendly certification path.

Grab the study materials
Modules, case study & practice questions.

Talk to an advisor
New to privacy and unsure where to start? Ask.