SPENCER WEST

London

GDPR in Practice

Common Mistakes, Key Risks and What Law Firms Need to Get Right

SPENCER WEST

Kristy Gouldsmith

I'm a data protection law specialist. I have years of experience in advising a wide variety of organisations across all sectors, including SaaS platforms, retailers, manufacturers, schools, care homes, financial services, law firms and property developers. I advise clients of all sizes, from small business to large American multi-national companies.

kristy.gouldsmith@spencer-west.com

07545 501200

SPENCER WEST

Introduction

“Most law firms don’t have a GDPR knowledge problem. They have a practical implementation problem.”

Firms usually know the basics but problems arise in:

- day-to-day behaviour,
- inconsistent processes,
- pressure situations,
- legacy practices,
- and misunderstanding risk.

The ICO doesn’t expect perfection.

What it expects is reasonable governance, sensible decision-making and evidence that you took compliance seriously.

SPENCER WEST

Outline

- The most common GDPR mistakes law firms make and how to fix them
- Key risk areas, including data breaches, subject access requests, and marketing compliance
- Practical steps to strengthen your firm’s data protection processes
- How to approach the GDPR in a way that supports your business, not slows it down

SPENCER WEST

Definitions

Personal Data

any **information** relating to an identified or **identifiable natural person** ('data subject')

an identifiable natural person is one who can be identified, **directly** or **indirectly**, by:

- name
- identification number
- location data
- online identifier
- physical, physiological, genetic, mental, economic, cultural or social identity

Processing

any operation or set of operations which is performed on personal data

such as collection, recording, organisation, storage, adaptation, retrieval, consultation, use, erasure or destruction

Controller

Law firms are controllers in relation to our clients.

Article 6 - Legal Basis

All data requires a legal basis.


Consent from an individual
Contract with an individual
Comply with a legal obligation
Vital interests
Public tasks
Legitimate interests

Legitimate interest

Can send marketing texts or emails without consent if:

- obtained the contact details in the course of a sale (or negotiations for a sale)
- only marketing your own similar products or services
- give an opportunity to refuse or opt -- when first collecting the details and in every message after that

Legal Obligation

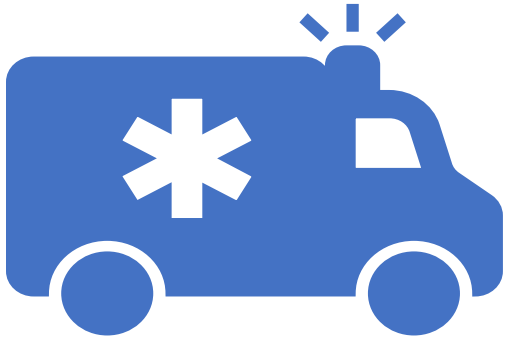
- We take proof of the right to work in the UK for employees.
- We do AML checks.
- We submit employee details to HMRC.

Contract

Used for data you need to process under a contract WITH AN INDIVIDUAL

Eg. Our engagement letter and terms of business

Vital Interests



If you have an accident at work and are unconscious, we will tell the ambulance crew if you have any medical conditions

Public interest

Some companies ask job candidates to fill out an equality and diversity questionnaire so that they can ensure that they are an equal opportunity employer.

This is a task in the public interest.

The most common GDPR mistakes law firms make and how to fix them

SPENCER WEST

A. Thinking that the GDPR is “an IT issue”

Data protection being treated as:

- an IT problem,
- or a compliance team problem,
- rather than an operational/legal risk issue.

“Most GDPR problems in law firms are people and process problems, not technology problems.”

Examples:

- fee earners bypassing processes,
- sharing documents informally,
- clicking on links in emails,
- uncontrolled spreadsheets.

Fix:

- governance ownership,
- practical policies,
- regular training,
- making compliance operational not theoretical.

SPENCER WEST

B. Over-retaining documents and emails

- “Just keep everything forever” mentality,
- Old archived files,
- Duplicate data,
- Former client information sitting everywhere.

Risks:

DSAR burden,

breach exposure,

cyber risk.

“If you don’t need it, don’t keep it.”

Example – 23 year old property files

SRA and law society do not set retention periods.

Fixes:

retention schedules,

defensible deletion,

matter closure processes.

SPENCER WEST

C. Treating SARs like litigation disclosure exercises

Common issues:

- over-reviewing,
- over-redacting,
- panic,
- inconsistent searches.

What's required:

- "reasonable and proportionate searches"
- not needing perfection,
- proportionality.

SPENCER WEST

D. Using email unsafely

Examples:

- autocomplete errors,
- wrong attachment,
- forwarding chains,
- failing to use BCC,
- sending sensitive documents unencrypted.

Fixes:

- delay send,
- encryption,
- checking attachments,
- internal reporting culture.

Key risk areas, including data breaches, subject access requests, and marketing compliance

SPENCER WEST

A. Data breaches

Most breaches are low-tech.
Human error dominates.
Cyber incidents are increasing but everyday mistakes remain the biggest issue.
Don’t be afraid of the ICO.

Examples:

- wrong recipient,
- attachment error,
- lost devices,
- clicking on links

Important:

- when to report,
- risk assessments,
- documenting decisions,
- importance of internal escalation.

A data breach is defined as a breach of security leading to the accidental or unlawful:

- Destruction
- Loss
- Alteration
- Unauthorized disclosure of
- Unauthorised access to

Personal Data

The rules…

- notify the ICO within 72 hours if the breach will result in risk to individuals

- notify individuals affected if the breach is likely to result in high risk to them

SPENCER WEST

B. Subject Access Requests

Why law firms struggle:

- large data volumes,
- mixed privileged/non-privileged material,
- emotionally charged requests,
- employment disputes,
- ex-clients.

Important:

- privilege exemptions,
- manifestly unfounded requests,
- timelines,
- documenting rationale,
- proportionality.

“A badly handled SAR often creates more risk than the original issue.”

“ Don’t panic – know the law”

B. Subject Access Requests

If you refuse to deal with a request because it is manifestly unfounded, then you must:

- tell the person making the request why it has been refused; and
- advise them of their right to complain to the ICO.

SPENCER WEST

Time limits

You must comply with a SAR without undue delay and within one month commencing when:

- You receive a request;
- Further information is needed to deal with the request (e.g. you processes a large amount of information concerning the data subject;
- You need to identify the requestor; or
- You're charging a fee for a manifestly unfounded request.

You can extend the time to respond by a further two months if the request is complex or if there are a number of them.

You must tell the data subject that you need more time within the first month and the reason why.

SPENCER WEST

The search

- You need to search for all data concerning the individual.
- This will be any digital files, paper files, emails, WhatsApp/Teams/ Slack messages and other data such as CCTV footage.
- The data subject is only entitled to the confirmation and personal data based on a reasonable and proportionate search.

SPENCER WEST

Redactions and Exemptions

Exemptions are listed in the schedules to the Data Protection Act 2018.

Examples are legal professional privilege, management forecasting or protection of the rights of others.

People have a right to receive copies of their own data but not business data or the data of other people.

SPENCER WEST

Legal Professional Privilege

The SAR provisions to do apply to personal data where it:

- is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),
- is necessary for the purpose of obtaining legal advice, or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights

SPENCER WEST

Who is the requestor – a third party, the client or an employee?

If the requestor is a third party, say a litigant in person on the other side, then pretty much everything falls under LPP. The exceptions will be things like:

- Your communications with the data subject
- Documents independently created – e.g. a motor vehicle accident report

If the requestor is the client, then they are entitled to request all of their personal data. This includes communications within the firm unless that advice falls within LPP e.g. the client is suing the firm and the firm is the client.

This means that emails between partners, for example, about the client, will be included in a SAR, unless they fall within the third party exemption

If the requestor is an employee, then you need to look at the third party exemptions and the management forecasting exemptions (a current redundancy process).

SPENCER WEST

C. Marketing compliance

Marketing:

- mailing lists,
- seminar invites,
- networking follow-ups,

Key issues:

- PECR,
- consent vs legitimate interests,
- unsubscribe mechanisms,

SPENCER WEST

Business to client - consent

When to use data consent in marketing- the opt-in (consent)

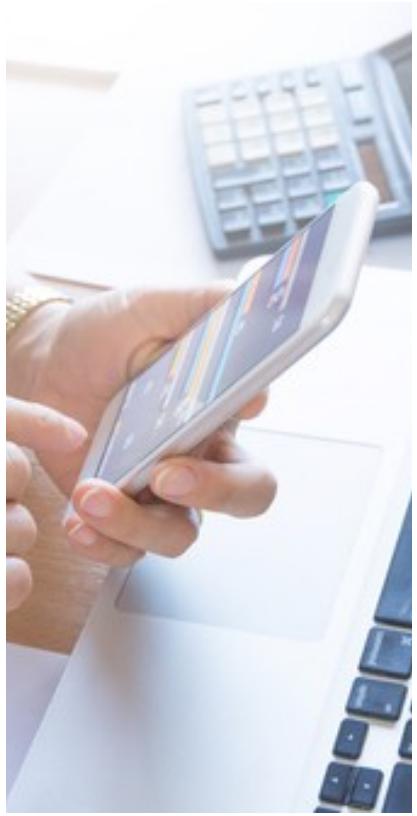
Consent is the legal basis for processing when you have not had any interaction with a person.

Use a tick box to ask a person if they would like to sign up to your newsletter, for example.

Consent is used when you have no relationship with the person.

SPENCER WEST

PECR



The rules are from the Privacy and Electronic Communications Regulations (PECR). The idea is that if an individual bought something from you **recently** or entered negotiations for a sale, that they are probably happy to receive marketing from you about similar products or services even if they haven't specifically consented.

So, organisations can send marketing texts or emails if:

- they have obtained the contact details in the course of a sale (or negotiations for a sale) of a product or service to that person;
- they are only marketing their own similar products or services; and
- they gave the person a simple opportunity to opt out of the marketing, both when first collecting the details and in every message after that.

SPENCER WEST

Business to client -- **CURRENT AND FORMER CLIENTS.**

Marketing using legitimate interest and an opt-out tick box is used with

(1) Existing and former clients and

(2) those who have begun ‘negotiations for a sale.

Used to contact former and existing clients to send marketing (unless they have opted out of receiving marketing from your firm. You must check.)

SPENCER WEST

B2B

A business email is considered to be personal data e.g. Kristy.gouldsmith@spencer-west.com

However, one business can send a marketing email to a personal business email address using the legal basis of legitimate interest.

You can have a marketing company do this work for you.

SPENCER WEST

D. Recording meetings & WhatsApp

AI note takers,

Messaging services.

Important:

- governance,
- approved tools,
- policies,
- training,
- human oversight.

SPENCER WEST

Recording meetings

Legal basis is **consent**

Why? Because you are gathering new data and recording the client (image, words and information about the client).

What do I do? You need to get consent from the meeting attendees before recording the meeting. If someone declines, then don't record the meeting or that person doesn't attend/speak etc.

Your privacy notice for clients should inform them that you may seek consent to record online meetings.

Training events are different – the legal basis is legitimate interest.

SPENCER WEST

Messaging Services

- WhatsApp and other messaging service messages are part of the client file

- In the case of MacInnes & Anor v DWF Law Llp [2025] EWHC 3252 (SCCO) (05 December 2025), the judge was assessing WhatsApp messages and stated:

“if you charged for it then it's part of the file”

Contract

Used for data you need to process under a contract between an individual and a controller

eg. Engagement letter and terms of business

You can’t make it a contractual obligation for the client to be recorded

Practical steps to strengthen your firm’s data protection processes

SPENCER WEST

A. Make GDPR operational

The best firms:

- embed GDPR into workflows,
- not separate compliance documents that nobody reads.

Examples:

- onboarding checklists,
- matter opening controls,
- standard templates,
- breach reporting process.

SPENCER WEST

B. Build a reporting culture

Culture:

people hiding mistakes,
fear culture,
delayed reporting.

“Your biggest risk is not the mistake. It’s the mistake nobody reports.”

If you don’t have any data breaches, it’s because either no one can recognise one or no one reports them.

SPENCER WEST

C. Train differently

Most GDPR training is:

- too generic,
- too theoretical,
- forgotten immediately.

Better approach:

short,

scenario-based,

law-firm-specific,

repeated regularly.

SPENCER WEST

D. Know your high-risk areas

Firms should identify the location and volume of data and do something about it:

- HR data,
- medical records,
- family law,
- criminal law,
- vulnerable client data,
- AML documentation.

Important:

Not all data carries equal risk.

SPENCER WEST

E. Governance and accountability

Important:

- documenting decisions,
- DPIAs,
- breach logs,
- policies,
- retention schedules,
- processor due diligence.

“The ICO looks for evidence of governance, not perfection.”

How to approach GDPR in a way that supports your business, not slows it down

SPENCER WEST

A. GDPR should enable trust

Good governance:

- wins clients,
- reassures insurers and regulators
- supports tenders,
- protects reputation

SPENCER WEST

A. Avoid “gold-plating”

Law firms often overcomplicate GDPR.

Important:

- unnecessary bureaucracy,
- over-lawyering decisions,
- endless forms,
- unrealistic controls.

SPENCER WEST

D. GDPR as a competitive advantage

Important:

- clients increasingly asking governance questions,
- supplier due diligence,
- vendor questionnaires,
- panel expectations.

“Firms that get governance right are increasingly more attractive to clients, insurers and regulators.”

SPENCER WEST

C. Proportionate risk management

Not every issue needs:

- a committee,
- external counsel,
- a 40-page DPIA.

Important:

- risk-based approach,
- proportionality,
- practicality

SPENCER WEST

Summary

- The most common GDPR mistakes law firms make and how to fix them
- Key risk areas, including data breaches, subject access requests, and marketing compliance
- Practical steps to strengthen your firm’s data protection processes
- How to approach the GDPR in a way that supports your business, not slows it down

Longbow House
20 Chiswell Street
London EC1Y 4TW

+44 (0)20 7925 8080
info@spencer-west.com

twitter.com/Spencer_West_
linkedin.com/company/spencer-west

Globally Connected, Locally Invested

spencer-west.com