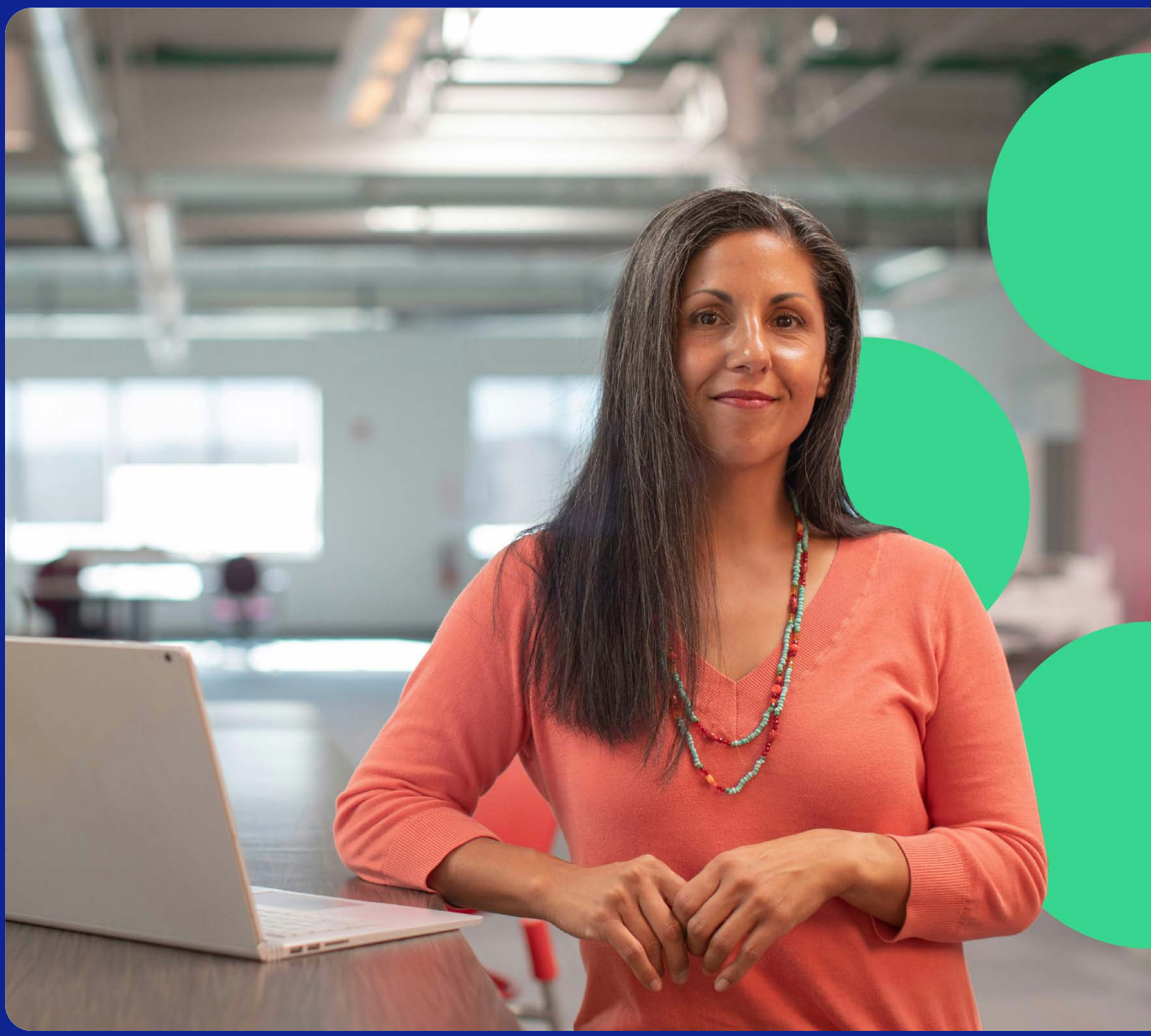
skillcast

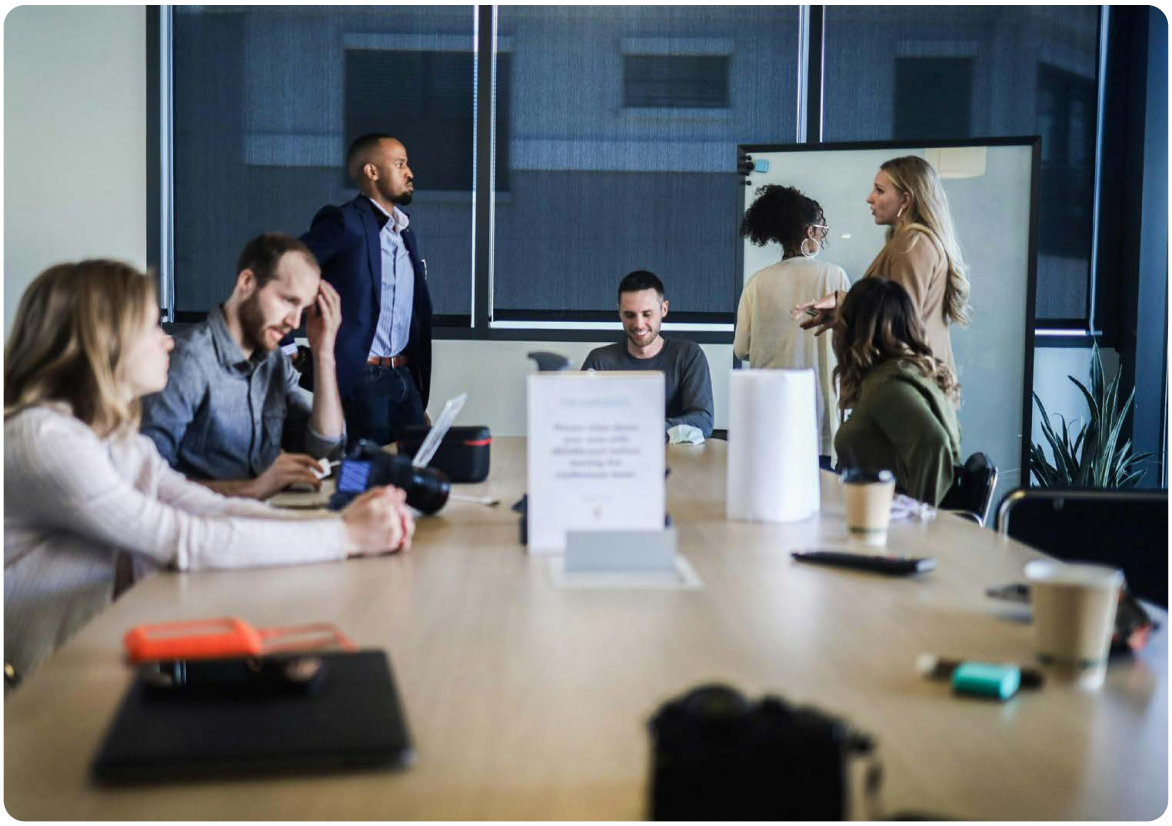
General Data Protection Regulation (GDPR) Toolkit



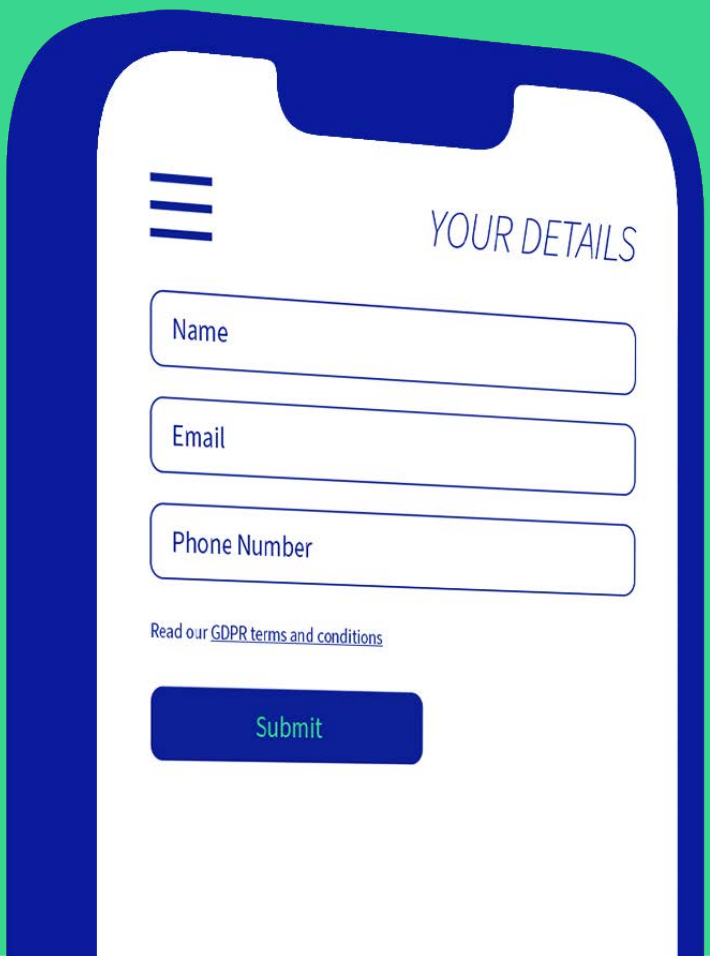
What is GDPR?

The sharing of personal data by organisations within Europe is subject to the General Data Protection Regulation (GDPR).

Under GDPR and other data protection laws, individuals are entitled to have their names removed from distribution lists. Comply with any such request promptly to avoid **GDPR sanctions**.



Subscribing customers, who trust companies with their personal and financial information, expect not just a product or service, but also the peace of mind that their data is secure.



GDPR Unpacked

Regulations under GDPR require you to train your employees to ensure they are aware of data protection risks, relevant legislation, their obligations under the law, the identity of the Data Protection Officer (DPO), and their responsibilities related to data breach reporting and handling Data Subject Access Requests (DSAR).

Widespread failures in meeting GDPR obligations have resulted in firms facing multi-million fines, emphasising the importance of maintaining compliance.

This toolkit provides resources to support your GDPR compliance efforts.

Did you know...

In 2024, Amazon France Logistique was fined €32m for its excessively intrusive monitoring system of employee activity.

Contents

Why GDPR Matters

Understanding the General Data Protection Regulation (GDPR) is essential for every organisation. GDPR is not merely a regulatory requirement - it is a comprehensive framework designed to safeguard personal privacy and build trust with stakeholders. Adhering to GDPR helps mitigate risks associated with data breaches, avoids substantial fines, and enhances your organisation's reputation.

By recognising and implementing GDPR principles, your organisation can:

- **Protect Individual Privacy:** Ensure personal data is handled responsibly, giving individuals control over their information.
- **Build Trust:** Strengthen your reputation and foster confidence among customers, partners, and stakeholders.
- **Avoid Legal Penalties:** Prevent severe fines and legal consequences associated with non-compliance.
- **Promote Best Practices:** Adopt robust data protection practices to enhance overall data security.
- **Support Business Growth:** Expand operations safely within the EU and UK, where GDPR is enforced.

Understanding the significance of GDPR equips your organisation to maintain compliance, protect its reputation, and uphold the trust of those you serve.

Cybersecurity Desk Aid

Staff Checklist

Always report issues promptly to IT, including unauthorised access attempts or malware, suspected data breaches, accidentally sharing sensitive information, and lost or stolen devices.

Don't hesitate to ask your IT department or security team for help if you're unsure.

Create strong, unique passwords
Mix lower and uppercase letters, numbers, and symbols. Avoid dictionary words and personal information, and do not reuse passwords.

Enable multi-factor authentication (MFA)
This adds an extra layer of login security, requiring a code beyond your password.

Never share your logins
This includes usernames, passwords, and security codes.

Keep work devices secure
Use strong passwords for screen locks, encrypt sensitive data, and update software regularly.

Don't mix personal and work use
Avoid accessing personal accounts and do not download unauthorised software on work devices.

Take care when accessing public Wi-Fi
Where possible, use a VPN for added security when connecting to public Wi-Fi networks.

Think before you download
Only download files from trusted sources. Be cautious of attachments, especially from unknown or unfamiliar senders.

Beware of social engineering
Don't share confidential or personal information in response to unsolicited calls, emails, or messages. It is a common technique used by fraudsters.

Beware of phishing attempts
Don't click on suspicious links or attachments in emails or messages. Be sceptical about links in branded emails. Always verify senders before responding.

Understand and follow data-sharing rules
Follow company policies on data handling, and don't share sensitive information without authorisation.

Information Security Checklist

Website Cookie Compliance

Cookie banners play a crucial role in ensuring organisations align with essential data protection regulations such as the UK GDPR and Privacy and Electronic Communications Regulations (PECR).

1. **Transparent cookie policy**
Users have the right to know how their data is collected and used. A transparent cookie policy builds trust and demonstrates respect for user privacy. Lack of transparency may result in user mistrust, damage to the organisation's reputation, and potential legal consequences.

2. **Prioritise consent for non-essential cookies**
Securing explicit consent is a foundational obligation according to GDPR. Prioritising consent for non-essential cookies guarantees adherence to the law. Neglecting to prioritise consent could result in unauthorised processing of personal data, infringing upon user privacy and inviting legal repercussions.

3. **Provide granular cookie controls**
Users should possess the capability to manage the categories of cookies they agree to. Granular controls empower users to make informed decisions regarding their privacy preferences. Insufficient user control could result in frustration and potential non-adherence to GDPR principles of fairness and transparency.

4. **Ensure prominence of the 'reject all' option**
Under GDPR, users have the right to decline cookies. A visible and explicit 'Reject All' option honors user choice and privacy. Concealing or downplaying the 'Reject All' option could invite allegations of deceptive practices and non-compliance.

5. **Storage limitation**
Cookie preferences might evolve, and users should have effortless means to modify their selections. Failing to manage cookie preferences adequately could result in user frustration, decreased engagement, and potential breaches of GDPR's principles regarding data accuracy and user control.

6. **Regularly audit & update policies**
Privacy regulations and cookie technologies are in a state of constant evolution. Conducting regular audits guarantees continuous compliance and adherence to the most recent legal standards. Outdated policies could inadvertently lead to violations, potential legal repercussions, and harm to reputation.

GDPR Training Aid

Self-Assessment Checklist

Assess the effectiveness of your GDPR procedures & controls

This comprehensive questionnaire will help you to assess your GDPR compliance effectiveness. You can both benchmark your existing processes and identify any missing GDPR procedures and controls.

Table of Contents

Section 1. Governance

The following questions relate to how well-prepared your governance and systems and controls are in respect of GDPR.

- Do you understand what personal and special categories of personal data mean to your firm?
- Do you have board support or endorsement for all matters relating to data protection and compliance with the GDPR?
- Do you have a new or revised data protection policy?
- Has a Data Protection Officer been appointed, with sufficient knowledge and experience and with autonomy to implement GDPR as required within your firm, and with direct access to the board (or equivalent)?
- Has a Data Protection Impact Assessment been completed, and a plan to address any deficiencies drawn up?
- Is your firm registered with the local data protection supervisory authority, and does your declared data use noted with them need to be updated or amended?
- Have you reviewed your usage and contracts with third-party suppliers and vendors to whom customer data may be passed, or who may have access to your systems which contain customer data?
- Do you have an appropriate data breach reporting procedure? Do your staff know how to report a breach and whom to report it to?
- Do you have a data breach response protocol in place? Establishing a pre-planned approach to the initial and ongoing management of a data breach?
- Are data breaches reportable via your whistleblowing process?

Section 2. Responsibilities

The following questions relate to your overall understanding of GDPR obligations.

- Do you believe that any employees reporting to you are aware of their obligations under GDPR?
- Do you believe that your peers in other key decision-making positions are aware of their obligations under GDPR?
- Do you understand what personal and special categories of personal data mean to your firm?
- Can you demonstrate that you have clear and explicit consent from your customers to hold and process the data that you hold now?
- Have you sent new fair processing notices to your customers, advising them of their new rights under GDPR, such as objecting or restricting processing, the right to be erased and the portability of their data?
- Have you established clear links with your marketing/product development areas to ensure privacy by design?
- Are you reviewing your website privacy terms and consents?
- Have you mapped a customer journey to identify all data touchpoints, enabling you to exercise a customer's right to be forgotten with ease and confidence?
- Have you a mechanism in place enabling breach identification and reporting within 72 hours of occurrence?

Section 3. Lawful Processing

The following questions relate to the lawful basis of processing personal data by your team:

- Do you understand where your customer data is?
- Do you know where your customer data comes from?
- Do you know how does customer data goes around the company and how it is shared?
- Do you know of all types of personal data being processed by your team and the purpose(s) of processing?
- Have you considered if this processing is necessary for the relevant purpose?
- Do you know of the lawful basis on which this data is collected and processed?
- Do you know whether the purpose(s) of processing and the lawful basis are documented in your privacy notice?
- In case the lawful basis of processing is Consent, are you sure that a record is being kept of when and how we obtained consent from the individual, and what they were told about how and why we would process their data at the time?
- Is customer consent obtained via a clear and standalone statement or document, rather than being part of a wider and unrelated set of terms and conditions or declarations?
- Have you got a process for notifying a customer that we need to change or add to the reasons that we currently process their data, explain why and obtain their consent for this change?

Section 3. Lawful Processing

- Do you know when and whom to ask for a data protection impact assessment (DPIA)?
- How do you manage data classification and communications? How is special category data treated compared to personal data? Are there any additional controls or access restrictions that you apply?
- Have you issued fair processing notices to your customers?
- Do you identify child account business separately from all other accounts?
- How are you demonstrating that where appropriate (aged 13 in the UK) that you have child consent for processing their data and that this consent is suitably informed?

Section 4. Data Security

The following questions relate to the security (confidentiality, integrity and availability) of the personal data is processed by your team:

- Would you be able to evidence that your team has taken measures to protect this personal data from external threats?
- Would you be able to evidence that your team has taken measures to protect this personal data from internal threats?
- Do you clearly communicate to your staff that data theft or misuse of customer data in any way is strictly prohibited and the consequences of such activity could be instant dismissal and even criminal prosecution?
- Do you have clear internal policies and training in relation to areas of computer misuse, electronic communications, safeguarding personal data on social media and information security?
- Do you have a record of who (departmental or individual) has access to customer data in your department and their need for this?
- How do you manage internal staff movement, cloned computer access and access revision and control? How is temp or contract workers computer access controlled?
- Does your internal training clearly demonstrate the serious impact of unauthorised data access or loss, by linking data theft, identity fraud, account take over and money laundering?
- Do you have a clear and easy-to-use breach reporting mechanism?
- Can one of your team report any concerns relating to data security, confidentially via your whistleblowing procedures?
- Do you have adequate firewalls and virus protection installed?

Section 4. Data Security

- Do you have clear password policies within your firm, i.e. required length, complexity and expiration times?
- Are controls such as clear desk policy and locked, confidential waste bins employed?
- Where are your servers located?
- What encryption protocols are used?
- Do you have a policy regarding the use of portable media devices and laptops and the procedures to be followed in the event of their loss?
- Do you have established protocols for home working, including the transportation of data to home sites?
- Is your data retention and destruction policy clear, and in line with the requirements of GDPR whilst being balanced against other potentially conflicting legislative requirements relating to data retention, such as the Money Laundering Regulations?

Section 5. Data Minimisation

The following questions relate to data minimisation and storage of the personal data that is processed by your team:

- Is there a review or sign-off of your application form/data collection mediums, designed specifically to confirm only essential data is collected, processed and stored?
- Do you know if a retention policy is being applied, i.e. this personal data is being erased once the purpose of processing is complete?
- Do you have a procedure in place, or could you satisfy a request from a customer to restrict the processing of previously obtained data, that is no longer considered necessary for the purpose of processing?
- How are you prepared to balance the requirement to only collect/process data that is limited to the purpose of processing, against other conflicting pieces of legislation?
- Are you and your staff equipped to identify information that is obtained, yet not necessary for the purpose of processing, and delete or cease the recording this information, for example, data revealed during a recorded telephone conversation with a customer, or notes made during a customer review, but upon reflection are not required?
- Where excessive data is noted as being present, yet is embedded within other relevant text or information, do you have methods of removing or redacting the unnecessary data? (Lord Sugar cheque as a bad example of redaction)
- Do you align your data collection and processing procedures against the lawful reasons of processing, i.e. to serve a legal or contractual obligation or being in the vital interests of the individual?

Section 6. Data Subject's Rights

The following relate to the rights of individuals whose personal data is processed by your team:

- Do you know if individuals are informed of the purpose and lawful basis under which the processing of their data occurs?
- How does this notification occur? (whether via our privacy notice or otherwise)?
- Is the notification in plain English, so understandable to the non-expert?
- Are your notifications (and other relevant information) available in translated format for non-English speaking customers and/or in other necessary formats such as Braille?
- Does your team have systems, procedures and training to comply with individuals' Right of Access?
- Have you removed any reference to a fee being charged for a data subject access request?
- To refuse to respond to a request would require you to prove to the requesting party that their access request was manifestly unfounded, who will be responsible for making such a decision?
- Where information that should be released under an access request is embedded amongst other customer's information, do you have means to either extract the relevant information or appropriately redact the non-relevant information? (Lord Sugar's cheque being an example of poor redaction)
- Does your team have systems, procedures and training to comply with individuals' Right to Rectification?
- GDPR requires that inaccurate data is rectified without undue delay, can your systems respond with efficiency to demonstrate this?

Section 6. Data Subject's Rights

- Are your staff trained to identify and balance the needs and requirements relating to rectification to other matters relating to retention, evidential purposes, for example? i.e. knowing when to rectify or not, or to seek guidance
- Does your team have systems, procedures and training to comply with individuals' Right to Erasure?
- Can you efficiently identify all electronic and paper-based records relating to a customer, no matter where and how it may be stored or located?
- Are your systems able to completely erase customer data?
- Are your staff trained to identify and balance the needs and requirements relating to erasure to other matters relating to required data retention, evidential purposes, for example? i.e. knowing when to erase and when not to, or to seek guidance
- How could you evidence to the data subject, if required, that their data has been deleted?
- Does your team have systems, procedures and training to comply with individuals' Right to Restrict Processing?
- Do your systems allow for the ringfencing of certain data or data sets, preventing that data from use?
- Are your staff trained and able to recognise the difference between a rectification, erasure, objection and restricted processing request?
- Do you have a checklist for staff use to review a restricted processing request against, which details the four reasons under which a subject can request a restriction of processing to ensure that processing isn't incorrectly or inappropriately restricted?
- Does your team have systems, procedures and training to comply with individuals' Right to Object?

Section 7. Data Breaches

The following questions relate to personal data breaches:

- Does your team have systems, procedures and training to recognise personal data breaches?
- Does your team know when and who to report personal data breaches within your Company?
- Does your company have a data breach response protocol, with consideration given to the following?
- Do you record the date, time and location of the breach and the date, time and location of when the breach was identified?
- Do you record the date and time that the appropriate breach notification procedure was invoked, including when a response protocol was initiated, such as response efforts?
- Do you know when to alert relevant personnel (including any external) to begin executing breach response protocols?
- Are you able to initiate relevant internal and external (data subjects, media, etc.) communications, where necessary, being advised by your legal and press departments? Remember what is or isn't said can have an impact on your reputation
- Can you secure any affected IT systems to preserve evidence and await any forensic analysis teams required?
- How can you minimise data loss/breaches and prevent further loss/breaches?
- Are you able to interview those involved in discovering the breach?

Section 7. Data Breaches

- Can you report to the police if necessary?
- Are you able to report to the data protection supervisory authority (within 72 hours of breach occurrence)?
- Can you notify senior management/board?
- Are you able to keep every step documented?
- At completion, can you debrief the response protocol to ensure it was efficient, sufficient and fit for purpose?
- Are you able to test the breach response protocols with a “mock” breach incident?

Section 8. Contractors & suppliers

The following questions relate to the use of contractors or vendor suppliers:

- Does your company use any contractors or vendor suppliers?
- Is any customer data transferred to, or accessible by these contractors or vendor suppliers?
- As part of your procurement process, does your company examine the supplier's data protection policy?
- Who in your company reviews such a policy? Are they experienced and sufficiently qualified to do so?
- Is there a data breach indemnity between your two firms? In whose favour does the indemnity run?
- Does your company have agreed protocols with the contractor or vendor supplier, detailing your expectations relating to data minimisation?
- Does your company have agreed protocols with the contractor or vendor supplier, detailing your expectations relating to how they would execute a data processing restriction?
- Does your company have agreed protocols with the contractor or vendor supplier, detailing your expectations relating to how they would execute a data objection notice?
- Does your company have agreed protocols with the contractor or vendor supplier, detailing your expectations relating to how they would execute a right to be forgotten?
- Is your contractor or vendor supplier located overseas? What is the adequacy of the data protection regime in that country?

Section 8. Contractors & suppliers

- Is your company the data processor? If so, are you clear on the requirements of your appointing data controller?
- Do your contracts with the contractors or vendor suppliers (or your appointed data controller) require updating?
- Does your company run any formal quality assurance programmes against the published data protection policy of the contractor or vendor supplier?
- Does your company run informal quality assurance testing of the contractor or vendor supplier data protection procedures, such as mystery shopping?
- Has your company an agreed data retention and data destruction policy with the contractor or vendor supplier?
- Does the contractor or vendor supplier's IT system allow for data portability?
- Is there a formal contract/processing review in place?

Section 9. Human Resources

The following questions relate to your HR department:

- Is your HR department aware that each employee is a data subject and that GDPR applies to the collection, processing, storage and deletion of employee data as well as customer data?
- Has your HR department mapped staff data in the same manner as this questionnaire requires for customer data? I.e. a data subjects rights, use of third-party contractors, minimisation of data, rights to object or restrict etc.?
- Are employees provided with a fair processing notice?
- Are employees able to object to their data being sent overseas to a parent or associated company with the group?
- Will your company need to use binding corporate rules for employee data processing?
- Will contracts of employment require amendment?
- Will your HR department need to obtain revised processing consent for all present and passed employees? Remember, they're considered to be processing data even if they are only storing it.
- Does or will your HR department view, use or consider content on employees' or future employees' social media sites, for purposes such as checking the legitimacy of sick days, or assessing character suitability for a role?
- Do your staff employment contracts allow for social media data to be used for commercial purposes?
- Do your job application forms or associated essential literature require consent from a potential employee to review their social media sites, and to use any information contained therein as part of recruitment?

Section 10. Overseas Data

The following questions relate to the transfer and/or processing of customer data overseas:

- Does your company transfer any customer data overseas?
- If yes, is the country of receipt within the EU?
- Does your company use any contractor or vendor suppliers?
- Does that company transfer customer any data overseas?
- If yes, is the country of receipt within the EU?
- Are binding corporate rules utilised?
- By what method is the customer data transferred overseas?
- Are appropriate robust encryption controls utilised?
- Is customer consent always sought and received before any overseas transfer of data exists, i.e. through a fair processing notice and consent declaration?
- What systems and controls exist around transfers of data overseas and which suitably experienced and qualified person reviews and authorises these controls?

Data Protection Principles

Understanding the seven data protection principles can help you ensure that personal data remains private and secure. It also keeps you on the right side of GDPR, avoiding potential fines, other regulatory action and reputational damage.

1 **Lawfulness, fairness, and transparency**

- Create a privacy policy that explains how you use, collect and process personal data.
- Make sure the people you collect data from can access the same information.
- Think about using a data protection impact assessment (DPIA) tool to help you identify and minimise the data protection risks of your project.

2 **Purpose limitation**

- Make sure your reasons for collecting and processing personal data are clear.
- Regularly review your data processing activities to ensure they're still necessary and relevant.
- Consider using a data mapping tool to identify the personal data you collect.

3 **Data minimisation**

- Data mapping tools can also help you spot unnecessary data, ensuring you only collect the data needed for your aims.
- Create a data minimisation policy setting out your processes for only collecting relevant data and who has access.

Data Protection Principles

4 Accuracy

- Use a data validation or verification tool to check data such as email and postal addresses, and phone numbers.
- Use a data cleaning tool to check for and remove duplicate or inaccurate info.
- Invest in data management system software, so you can monitor and manage data effectively and efficiently.
- Where it's possible – and completely secure – give people the ability to update their own information.

5 Storage limitation

- Include how long you keep data in your privacy policy.
- Use a data mapping tool to identify data that's no longer needed.
- Think about using cloud-based storage for ready-made security, plus quick and easy access for removing data.

6 Integrity and confidentiality

- Make sure your encryption tools are the latest versions. Check regularly for upgrades or patches.
- Continually and regularly back up your files, so you can recover your data in the event of fire or flood, for example.

7 Accountability

- Keep a record of your data processing activities using your own or a ready-made template available online.
- Consider appointing a dedicated Data Protection Officer to oversee your data protection practices.
- Provide data protection training covering the seven principles to promote understanding and support best practice.

Training Aid

Email Phishing Checklist

There are no fool-proof methods to prevent phishing. But you can reduce the risk by installing anti-phishing tools and making your employees aware of the risks.

Workplace malware protection tools may not always succeed. That's why it is important to try and avoid the risks by following a few simple guidelines.

1. **Keep your software up-to-date!**

   Ensure that you keep the software updated and mitigate the consequences of any mistake you might make.

2. **Be sceptical about links in branded emails**

   If you receive an email from a recognised brand, be sceptical if it asks you to click a link, provide your personal information or passwords.

3. **Avoid oversharing personal information on social media**

   Avoid sharing your position, job title, location, company and even age on social media.

4. **Train yourself to recognise personal styles**

   Make yourself familiar with how colleagues and suppliers communicate with you.

5. **Notify your IT team of suspicious emails**

   If you are suspicious of an email, then forward it to your IT team.

6. **Be wary of requests from generic addresses**

   If you receive an email from a generic address, e.g., customerservice@, help@, hr@ itsupport@, or payroll@, always be suspicious.

7. **Know the red flags**

   Be wary of generic greetings, unusual sender information, poor formatting, spelling/ grammar mistakes, dire warnings, incorrect facts, financial rewards or penalties and a lack of legally required links to subscribe.

8. **Finally, trust your instincts**

   If it sounds too good to be true, it usually is. If it sounds too bad, it also usually is. Cybercriminals are experts at making up extreme scenarios.

Training Aid

DSAR Preparation Checklist

The Information Commissioner's Office (ICO) has created two useful checklists to help you prepare for and deal with DSARs.

Preparing for subject access requests

- Know how to recognise a subject access request and understand when the right of access applies.
- Have a policy for how to record requests you receive verbally.
- If necessary, understand what steps you need to take to verify the requester's identity.
- Understand when you can pause the time limit for responding if we need to ask for clarification.
- Understand when you can refuse a request and know the information you need to provide to individuals when you do so.
- Understand the nature of the supplementary information you need to provide in response to a subject access request.
- Have suitable information management systems in place to allow you to locate and retrieve information efficiently.

Complying with subject access requests

- Have processes to ensure you respond to a subject access request without undue delay and within one month of receipt.
- Understand how to perform a reasonable search for the information.
- Understand what you need to consider if a third party requests on behalf of an individual.
- Be aware of the circumstances in which you can extend the time limit to respond to a request.
- Understand how to assess whether a child is mature enough to understand their rights.
- Understand that there is a particular emphasis on using clear and plain language if you disclose information to a child.
- Understand what you need to consider if a request includes information about others.
- Be able to deliver the information securely to an individual and in the correct format.

Training Aid

PCI DSS Checklist

PCI DSS is a set of standards designed to improve card data security. There are six goals and 12 requirements. To ensure PCI compliance, companies must have a rigorous and robust security policy. This requirement is often presented at the end of the PCI DSS framework, but it is the basis of all PCI DSS compliance.

- **Requirement 1:**
  Install & maintain a firewall
- **Requirement 2:**
  Don't use defaults for system passwords & other security parameters
- **Requirement 3:**
  Protect stored cardholder data
- **Requirement 4:**
  Encrypting the transmission of cardholder data
- **Requirement 5:**
  Use and regularly update anti-virus software
- **Requirement 6:**
  Develop and maintain secure systems and applications
- **Requirement 7:**
  Restrict access to cardholder data by business need to know
- **Requirement 8:**
  Assign a unique ID to each person with computer access
- **Requirement 9:**
  Restricting physical access to cardholder data
- **Requirement 10:**
  Track and monitor all access to network resources and cardholder data
- **Requirement 11:**
  Test security systems and processes
- **Requirement 12:**
  Maintain an information security policy

Posters

Print and share these with your staff and organisation

GDPR Awareness Personal Data

Everyone has the right to privacy and to have their personal data handled properly.

Our Company is committed to protecting your personal data as well as that of our customers, suppliers, and everyone we work with. Help us meet this commitment. Make sure you know what personal data is and what your responsibilities are. **Examples include: A customer's name. Their date of birth. Their postal address. Their IP address.**

79% **don't know your date of birth is personal data**

10% **of firms don't protect the customer's email address**

56% **of firms don't know email marketing lists are personal data**

29% **don't think they have to protect a customer's address**

SPEAK UP!
Contact our confidential whistleblowing team to report data breaches

Source:
TrendMicro & Opinium

skillcast

GDPR What do you know?

Follow these top tips and help your business comply with the UK General Data Protection Regulation.

Awareness Make everyone aware of the laws on data protection and explain how they will impact them.

Documentation Know what personal data you collect, store and share — and where it flows.

Privacy policy & notices Ensure they explain why data is used, for how long and user rights.

Individual rights Be ready to respond to access, deletion or objection requests within a month.

Consent Record, manage, and prove consent for all data use where required.

Data Protection Officer (DPO) Appoint a DPO if processing large-scale or sensitive data.

International transfers Understand and document where data goes and ensure lawful transfer.

Breaches Have processes to detect, report and handle data breaches within 72 hours.

Don't leave it too late Breaches damage trust and are expensive — be prepared before it happens.

Data Subject Access Requests Respond to DSARs within one month, free of charge.

skillcast

GDPR Special Category Data

Some personal information is inherently more sensitive and under UK/EU GDPR, it's subject to stricter protection rules.

Racial or ethnic origin
Reveal a person's heritage - misuse risks discrimination.

Political opinions
Could affect employment, services or profiling.

Religious or philosophical beliefs
Highly sensitive beliefs - must not be exposed.

Trade-union membership
Linked to workplace and political identity.

Genetic data
Unique and unchangeable - poses lifelong privacy risk.

Biometric data Used for identification - if leaked, it can't be reset.

Health data
Reveals medical conditions and personal vulnerabilities.

Sex life or sexual orientation
Deeply personal - misuse may cause stigma.

Handling special category data comes with greater responsibility — **protect it with care.**

To learn more, visit the official UK Information Commissioner's Office (ICO) guidance: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources

skillcast

GDPR Awareness

Fundamental Rights

Understanding GDPR isn't just a legal requirement—it's about respecting people's fundamental rights in a data-driven world.

These rights give individuals control over how their personal information is used, helping to build trust, transparency, and accountability.

Fundamental GDPR rights:

- The right to be informed
- The right of access
- The right of rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights on automated decision making and profiling

Our company is fully committed to ensuring the data protection rights of all individuals under the General Data Protection Regulation (GDPR).

72 hours. The time we have to notify of any data breaches.

1 month. The time we have to respond to data requests.

Up to €20m. This is how much we could be fined for breaching the GDPR rules.

skillcast

GDPR Training: Why It Matters

Training isn't a tick-box exercise, it's your frontline defence.

With data breaches, phishing scams, and regulatory changes on the rise, every team member plays a vital role in protecting personal data. Ongoing GDPR training keeps everyone sharp, informed, and compliant.

What Can Go Wrong Without It?

- Accidental breaches due to outdated knowledge
- Poor data handling that puts individuals' rights at risk
- Missed phishing threats that lead to cyberattacks
- Unlawful communication practices that breach PECR
- Reputation damage and regulatory fines — up to 4% of turnover

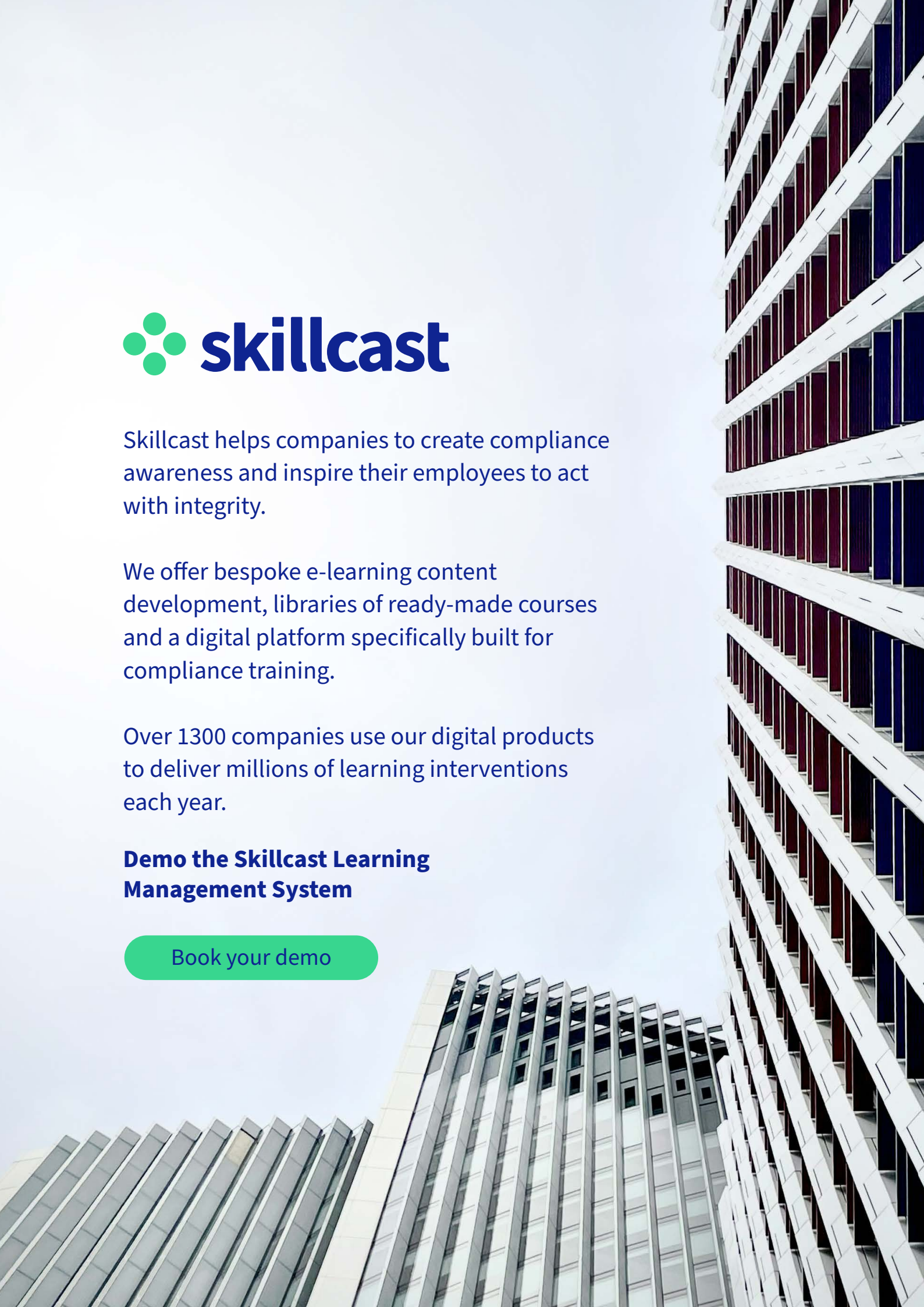
What Should Training Cover?

- Data Protection Basics – How to collect, use, and store personal data safely
- Phishing Awareness – Spotting and avoiding common cyber traps
- Cybersecurity Fundamentals – Reducing everyday risks at work
- Information Security – Why business data must be protected
- Social Media Use – Avoiding risky posts and behaviours

Keep Learning, Stay Protected

GDPR is evolving — so your knowledge should too.
Learn more about our GDPR training at skillcast.com/GDPR

skillcast



skillcast

Skillcast helps companies to create compliance awareness and inspire their employees to act with integrity.

We offer bespoke e-learning content development, libraries of ready-made courses and a digital platform specifically built for compliance training.

Over 1300 companies use our digital products to deliver millions of learning interventions each year.

Demo the Skillcast Learning Management System

Book your demo