



GDPR: A GUIDE FOR ECOMMERCE

HEATHER BURNS & DAN BARKER

FOR ECOMMERCEGUIDE.COM

INTRO

This guide aims to help Ecommerce businesses understand one of the most important, yet most confusing, legal requirements to have come into force since online retail took off: GDPR, the ‘General Data Protection Regulation’.

It is likely that you have read some of the higher profile details of GDPR (it’s been hard to miss): The fact that it applies to any company dealing with any data related to EU or UK customers; the *maximum* level of fines up to €20 million, or 4% of annual global turnover (‘whichever is higher’) for companies in breach of the regulation.



You may also have read general guides on GDPR. Whereas general guides tend to cover all areas of the GDPR at an extremely high level, this guide aims to take the most important elements of the regulation for *ecommerce* businesses, giving you an overview and an understanding of how it maps to your business, and your responsibilities.

Most literature related to GDPR tends to fall into one of two buckets:

- Extremely high level – short blog posts, infographics, etc.
- Extremely granular – eg. The text of the regulation itself.

This guide aims to fill the gap in between these extremes and, though it would be useful to most readers, it aims to cover areas more specific to Ecommerce companies.

ABOUT THE AUTHORS

	<p>Heather Burns is a digital law and tech policy specialist. She helps digital professionals get to grips with tech regulations and political issues, most specifically those that affect web design and development. You may hire her for research, speaking, writing, or consulting at webdevlaw.uk or on Twitter at @webdevlaw</p>
	<p>Dan Barker has worked in ecommerce for 20 years. He has worked for over 100 brands, from short consulting projects to CMO and board positions. You may find more information about him at barker.co.uk or on Twitter at @danbarker</p>

ABOUT ECOMMERCEGUIDE.COM

EcommerceGuide.com offers information and guidance related to all aspects of Ecommerce. The site features a range of guides, alongside the largest independent Twitter account dedicated to Ecommerce, with tens of thousands of followers at: [@ecommerce](https://twitter.com/ecommerce).

- Visit the site at <https://ecommerceguide.com>
- Follow EcommerceGuide on Twitter at <https://twitter.com/ecommerce>

CONTENTS

Intro	2
About The Authors.....	3
About EcommerceGuide.com	3
What is GDPR?	6
The New Rules	7
The Data Protection Act, GDPR, and 'Personal Data'	7
Personal Data	7
Sensitive Personal Data	8
Expanded types of Personal Data	9
Who GDPR affects	10
GDPR & Brexit	10
GDPR for Ecommerce - 11 key areas & checklists	13
11 Key Areas	13
GDPR for Ecommerce - Area 1: Awareness	14
Awareness: 6 Key Questions to Ask	15
GDPR for Ecommerce - Area 2: Privacy Notices	16
Plain English; Open Information	16
Privacy Notices & Third Parties	16
Privacy Notices: 8 Key Questions to Ask	17
GDPR for Ecommerce - Area 3: Individual rights	18
Individual Rights: Key Questions to Ask	19
GDPR for Ecommerce - Area 4: Subject access requests	20
Subject Access Requests: 9 Key Questions to Ask	20
GDPR for Ecommerce - Area 5: Data Collection - Information you hold	22
Data Collection: Key Questions to Ask	23
GDPR for Ecommerce - Area 6: Consent and legal basis	24
Legitimate interests?	26
Soft opt in?	27
Consent & Legal Basis: 8 Key Questions to Ask	28
GDPR for Ecommerce - Area 7: Ecommerce Businesses Dealing with Children	29
Dealing with Children: 7 Key Questions to Ask	29
GDPR for Ecommerce - Area 8: Data breaches	30
Data Breaches: 6 Key Questions to Ask	31
GDPR for Ecommerce - Area 9: International and Privacy Shield	32
International Issues: 6 Key Questions to Ask:	33
GDPR for Ecommerce - Area 10: "Privacy by Design" & "Data Protection by Default"	34
Privacy By Design: 7 Key Questions to Ask	35
GDPR for Ecommerce - Area 11: Data Protection Officers	37
Do You Need a Data Protection Officer?	37
The Role Of A DPO	38
Data Protection Officers: 6 Key Questions to Ask	39



GDPR FOR ECOMMERCE: AN OVERVIEW

WHAT IS GDPR?

Despite much coverage, there is still a very low level knowledge around what specifically GDPR is, and where it came from.

In summary: GDPR is a complete update and overhaul of the existing EU data protection regime – ie. It is an update of earlier work, not something entirely new - which dates from 1995. Its provisions affect EU countries, *and* any business selling to an EU country.

Even the UK, where there is much confusion over what Brexit means from a legal point of view, the one single point of legal certainty is GDPR - it will carry through the UK's transition out of the European Union and beyond.

On **25 May 2018** the EU's General Data Protection Regulation (GDPR), the successor to the Data Protection Act, became enforceable across Europe, including the UK.

THE NEW RULES

For ecommerce businesses, the new rules will mean a new set of rules to follow, affecting in the main the following four data-related practices:

1. The data you collect;
2. The ways you use the data;
3. The ways you store the data; and
4. The ways you share the data.

THE DATA PROTECTION ACT, GDPR, AND 'PERSONAL DATA'

GDPR replaces the existing data protection regime, 1995's EU Data Protection Directive. (In the UK this was known as the Data Protection Act of 1998, the year in which it was given 'Royal Assent' in the UK, before coming into enforcement in 2000).

Though there have been many changes to specific areas of data law since, GDPR is by far the most significant update following the now 20+ year old Data Protection Directive.

PERSONAL DATA

GDPR, and the EU's principles of data protection and privacy in general, pertain to what they (and we) refer to as '**personal data**'.

Personal data, for our purposes, means information about a living individual who could be identified from that data, either on its own *or when combined* with other information. GDPR officially defines personal data as:

"any information relating to an identified or identifiable natural person."

For an Ecommerce company, that is likely to mean the following: Your customer records, information gathered in relation to recognisable *potential* customers, and the data that people generate using or accessing your websites, apps, and other services, are **personal data**.

It is worth knowing that – in GDPR terms – ‘personal data’ is broader than some companies may self-define. For example, IP addresses, and Cookie identifiers are specifically mentioned:

“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as **internet protocol addresses**, **cookie identifiers** or other identifiers such as radio frequency identification tags.

This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.”

In response to this, Google, for example, have produced an ‘EU user consent policy’ notifying advertisers they must obtain consent for "the collection, sharing, and use of personal data for personalization of ads". Elsewhere, they define personalized advertising as “targeting features, including remarketing, affinity audiences, custom affinity audiences, in-market audiences, similar audiences, demographic and location targeting and keyword contextual targeting”.

SENSITIVE PERSONAL DATA

Beyond personal data there is also **sensitive personal data**, which is defined as any information concerning an individual’s:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life or sexual orientation
- Past or spent criminal convictions

Sensitive personal data requires stricter curation, and the loss or breaches of such data rightfully carries stricter punishments.

EXPANDED TYPES OF PERSONAL DATA

GDPR **expands the definition of personal data** from the 1995 standard to include an individual's:

- Genetic data
- Biometric data
- Location data
- Online identifiers

The processing of sensitive personal data must meet at least one of the following conditions:

- The explicit consent of the data subject;
- The subject has expressly made their information public (such as a political blog);
- The data is necessary for religious or trade union purposes;
- Certain health reasons;
- The data is necessary for employment, social protection, a legal claim, or a similar public interest;
- Certain archival reasons.

The 1995 data protection principles established that personal data must be:

- Processed in a manner which is fair and lawful;
- Used only for the manner in which it was intended to be used;
- Processed in a manner which is adequate, relevant, and not excessive;
- Accurate and kept up to date;
- Not kept for longer than its intended purpose;
- Processed in accordance with the rights of the people the data is about;
- Protected by technical and organisational security measures;

- Not transferred to third countries outside the EU which do not guarantee an adequate measure of data protection.

GDPR continues these principles, expands upon them, and adds additional responsibilities.

WHO GDPR AFFECTS

If you do business in the UK or across the European continent, GDPR and its requirements apply to you and your work. As an example, if your business is geographically located within the United States, but you provide ecommerce functionality to customers in the United Kingdom or European Union, GDPR applies to those elements of your business.

Data protection law applies to all personal data about individuals collected or processed in Europe regardless of those individuals' nationality or citizenship. It applies whether the data is on paper or stored electronically.

Data protection law also applies across all sectors, industries, and situations.

There is no minimum size a business must be before the law applies; sole traders must work to the guidelines just the same as large corporations.

In the lead-up to GDPR, many industry groups and trade bodies are developing guidelines for their members which go above and beyond the baseline required by the legislation. If you belong to an organised industry, please check with your industry body.

GDPR & BREXIT

We have already discussed how GDPR will remain the law, and the standard to achieve, for at least several years to come across the EU. The question that follows is what will happen to data protection law in the UK in the years after Brexit.

In September 2017 Parliament began drafting a Data Protection Bill which could form the bridge between GDPR and any future privacy regime. As detailed in the 2017 Queen's Speech, the Bill would "ensure that our data protection framework is suitable for our new digital age, and cement the UK's position at the forefront of technological innovation, international data sharing and protection of personal data".

That, of course, is the spin. In truth, as of this writing, the proposals are very close to what the UK was getting under EU GDPR anyway, packaged as the Government's own idea.

In practice, the actual work will be a bit messier than that.

For ecommerce businesses, it is imperative that any post-EU UK data protection regime remain fully equivalent to European data protection standards. Without equivalence, the most basic data flows will become contentious, cumbersome, and expensive. Ecommerce professionals must be prepared to make our industry's needs clear to government in the years to come.



GDPR: 11 KEY AREAS FOR ECOMMERCE, & CHECKLISTS

GDPR FOR ECOMMERCE - 11 KEY AREAS & CHECKLISTS

The following 11 sections cover the fundamentals of GDPR compliance specifically as they pertain to ecommerce businesses.

GDPR is an enormous topic. This guide is by no means comprehensive, nor is it legal advice. As an ecommerce professional, or someone wishing to understand the requirements of ecommerce businesses under GDPR, it is designed to give you the means to identify key issues to tackle or ensure you have addressed.

11 KEY AREAS

The 11 key areas we have broken out are as follows:

1. Awareness
2. Privacy Notices
3. Individual Rights
4. Subject Access Requests
5. Data Collection - the Information You Hold
6. Consent & the Legal Bases
7. Ecommerce Businesses Dealing with Children
8. Data Breaches
9. International Issues & Privacy Shield
10. "Privacy by Design" & "Data Protection by Default"
11. Data Protection officers

Each area provides an overview of GDPR as it relates to ecommerce companies, followed by a checklist of 'Key Questions' to ask in order to inform your organisation's compliance.

GDPR FOR ECOMMERCE - AREA 1: AWARENESS

The most basic step involved in GDPR compliance is **awareness** of the regulation and what it will mean for your ecommerce business. The simple fact that you are reading this (and, hopefully, will keep reading to the end) has already put you at an advantage.

You can create a healthy culture of respect for data protection and privacy by making everyone you work with aware of the ways the law is changing and how these changes will impact your work in a positive way.

This includes the people you work with within your business as well as third-party contractors and service providers.

Internally, devising a GDPR awareness and implementation plan for everyone on your team, ranging from senior management to software developers. Make sure everyone understands what GDPR carries over from the old Data Protection Act and what requirements are new.

Awareness has no shortcuts, so you should allocate appropriate human and technical resources to the process both before and after May 2018. Remember that your compliance requirements are not a one-off task: they must be incorporated into ongoing processes and functions.

A thorough approach to implementation would involve regular reports on your progress to your senior management and Board, with the expectation that they would provide healthy scrutiny and pushback throughout the process.

Externally, you should speak with your contractors, partners, and third-party suppliers about their own GDPR plans as well, particularly if your business relationship involves the exchange of data. Under GDPR, in the event of a regulatory concern, *each* controller or processor is held liable for the entire damage. That means that complete compliance on your side, but incomplete compliance on the part of a party which handles your data, will still rebound onto yourself. For retailers, this has a lot of ramifications. Your email marketing platform contains your customers' personal data, often remarketing technology providers

will contain this, your CRM provider likely stores your customers' personal data, if you use a cloud-based ecommerce platform, the cloud provider (of course) records your customers' personal data on your behalf.

It may well come to pass that compliance forces you to renegotiate your contracts, modify your data exchanges, and renegotiate service agreements. In the event of any instance of outright resistance to compliance from, for example, non-EU service providers who refuse to acknowledge that GDPR applies to them, you must end the commercial relationship and source a new third party service provider.

AWARENESS: 6 KEY QUESTIONS TO ASK

1. Do you understand what GDPR continues from the old Data Protection Act, and what is new?
2. Are you confident that you are compliant with the existing Data Protection Act?
3. Have you devised a GDPR awareness and implementation plan for all employees, ranging from senior management to line staff?
4. Are you providing your Board with regular updates about your GDPR implementation progress?
5. Have you allocated appropriate human and technical resources to GDPR implementation?
6. Have you spoken with your contractors and suppliers about their own GDPR implementation plans?

GDPR FOR ECOMMERCE - AREA 2: PRIVACY NOTICES

Under the previous data protection regime, privacy policies became long, lazy, and legalistic. Their main beneficiaries were often solicitors who charged thousands of pounds to generate them from templates, and the end results rarely had close relevance to the site or the privacy issues within it. A litany of privacy issues on sites which had privacy policies longer than novels also hinted at the use of policies as vehicles to *violate* privacy, not protect it.

GDPR aims to reclaim privacy notices as concise, transparent, and intelligible dialogues with your users. They also represent the public face of GDPR's move towards granular consent and user empowerment. Becoming a customer, or adopting a service, is no longer a means for retailers to achieve other ends.

PLAIN ENGLISH; OPEN INFORMATION

Going forward, your ecommerce business's privacy notices need to be written in plain English. They need to contain certain kinds of information in a cleanly formatted manner. And everything you are doing with your users' data - *everything* - needs to come out into the open. What are you doing with the data? Why do you collect it? What is your consent or legal basis for holding the data? Who do you share it with? Where is it stored? Are you transferring the data outside the EU? How can a user invoke their individual rights?

Design also comes into play here. Privacy information notices should be presented in an attractive way, preferably a table with icons. (Many European data protection regulators are developing standardised templates for adoption in the leadup to May 2018).

PRIVACY NOTICES & THIRD PARTIES

Crucially for ecommerce businesses, privacy notices must list all third parties who receive your data, and what *they* do with it. This means *all of them*: PayPal's GDPR-ready privacy notice includes over 600 third party providers grouped by service. It works the other way: you must indicate what data you receive *from* third parties, whether that is payment verification information or information from advertising beacons.

Your privacy notice details on third party providers need to make clear which services are essential (for example, payment processors) and which are for analytics, advertising, and marketing purposes. Responsible development would include links to each third party's own privacy policy within your privacy statement, giving your users a means to opt out of individual tracking at source.

It is vital to review the public privacy notices of your third-party service providers, particularly those who receive or use your data. Take note of any providers which have not updated their notices to the new format; take heed of any providers which *will* not.

PRIVACY NOTICES: 8 KEY QUESTIONS TO ASK

1. Have you reviewed the privacy notices on your web sites, apps, and online services, as well as any printed literature you display at events, for currency, accuracy, and compliance with the 2018 (not 2008) guidelines?
2. Can you ensure that your privacy notices are:
 - a. Written in plain English, with no "legalese";
 - b. Broken down into clear sentences and short paragraphs;
 - c. Provide an honest description of what data is collected, how data is processed, how data is used, who data is shared with, and what the user's rights are;
3. If not based on consent, do your privacy notices explain your lawful basis for processing user data?
4. Do your privacy notices list all third party partners and services providers with whom you share data, and note what that data is and how it is used?
5. Do your notices inform users about their rights, including who to contact for a subject access requests, and how they can complain to a regulator (in the UK, ICO) if they feel you are not honouring their data?
6. Do your notices provide clear granular options for consent, individual rights, and subject access requests?
7. Do your notices provide clear contact details for your company, your point of contact for subject access requests, and your data protection officer, if applicable?
8. Have your notices separated your privacy standards from general terms and conditions, particularly on your web sites and apps?

GDPR FOR ECOMMERCE - AREA 3: INDIVIDUAL RIGHTS

Under GDPR, the rights that individuals have over the collection and processing of their personal data are greatly expanded. For your ecommerce business, this means respecting those rights, implementing them into your planning structures, and being prepared to meet users' invocation of these rights in an open and fast way.

The rights that individuals have over their data include:

- The right to be **informed** about what you are doing with data through privacy notices, as we have previously discussed;
- The right of users to **access** a copy of the data you hold on them;
- The right to **correct** any erroneous data that you hold;
- The right to **erasure**, meaning the right to request that you delete certain kinds of data that you hold, commonly known as the "right to be forgotten";
- The right to **restrict processing**, or the right to ask you to stop using their data in certain ways;
- The right to **data portability**, or the right to take the data you hold about them to another service provider;
- The right to **object** to your uses of their data; and
- Their rights in relation to **automated decision making and profiling**, including data you use or share for the purposes of advertising, marketing, and behavioral analysis.

For ecommerce businesses, the latter requirement is most likely to have the largest impact. Users can object to their data being shared with marketers. They can also object to data being passed in the background for profiling purposes.

Your privacy notices should include information on how your users can invoke these rights over their data, and your business should - of course - have the mechanisms to carry this out.

It is critical to remember that these rights are **granular**. For example, a customer can object to your sharing their data with third parties for advertising purposes. This cannot impact any other aspect of your commercial relationship.

INDIVIDUAL RIGHTS: KEY QUESTIONS TO ASK

1. Have you reviewed your current provisions for meeting individual rights?
2. Have you reviewed how you publicise individual rights in your privacy notices?
3. Have you determined which data you hold could be subject to these rights?
4. Do you have the technical capabilities to produce an electronic copy of the data you hold on a user?
5. If applicable, does your product or service have the the technical capability for data portability?
6. Have you unbundled individual rights over data used for automated decision making and profiling from the data which is strictly necessary for the provision of your services?
7. Are you aware that you cannot charge users any administrative fee for invoking these rights, or any costs for the time you require to meet them?

GDPR FOR ECOMMERCE - AREA 4: SUBJECT ACCESS REQUESTS

We have already spoken about the enhanced rights that your customers and clients have over their data under GDPR. The simplest way that they can invoke these rights is called a subject access request (SAR).

This is a request made by someone whose data you hold or process, submitted in any format, for you to provide them with

1. Confirmation that you are processing their data;
2. A copy of the personal data that you hold on them;
3. Any other information you have in your possession about the subject, including what the data you have passed to third parties, and what basis this was done under.

A subject access request is a user's first step in invoking the other individual rights they have over their data. Your Subject Access Request process should be clearly explained in your privacy notices, which we will discuss later.

Your business must respond to a subject access request within one month of receipt. Because a subject access request is an invocation of fundamental rights, you cannot charge individuals an administrative fee or surcharge to exercise this right.

SUBJECT ACCESS REQUESTS: 9 KEY QUESTIONS TO ASK

1. Have you created an Subject Access Request process?
2. Is your Subject Access Request process detailed in your privacy notices?
3. Is your internal Subject Access Request process documented in a way that would meet your data protection regulator's approval?
4. Do you have a central point of contact for handling subject access requests?
5. How are SARs tallied in your organisation? Who is informed of their receipt, their progress, and their completion?

6. Do you have the technical and staffing capability to respond to subject access requests within 30 days?
7. Are your systems equipped to generate the data required under an SAR?
8. Does your documentation ensure that no uses of data would be overlooked when responding to an SAR?
9. Do your third party subcontractors and partners have a documented and visible Subject Access Request process?

GDPR FOR ECOMMERCE - AREA 5: DATA COLLECTION - INFORMATION YOU HOLD

The most fundamental step towards GDPR compliance is being constantly aware of *what* personal data your business holds, *why* you collect it, *where* it is stored, and *who* you share it with.

You should audit all of the data collecting and processing activities you carry out in your business. It is entirely likely that the process of carrying out this audit will identify activities you no longer do, processing you no longer perform, and information you no longer need. This process - the first step towards data minimisation and deletion - is also a step change under GDPR.

This audit should include the data you receive and process from third party providers. Even if the data is only passing through you in transit, you have a responsibility to know what it is and how you are safeguarding it.

For most ecommerce businesses, data collection and processing is regular, includes sensitive personal data, or could threaten people's rights and freedoms. For these reasons, the audit of the data you hold should include a full record of all of your data collection and processing activities, including:

- The purposes for which you are collecting and/or processing personal data;
- A description of the categories of individuals you are processing data about;
- A description of the categories of data you are processing;
- A description of the recipients of personal data you are transferring out of your organisation;
- A description of international (non-EU) transfers of personal data, including what safeguards are in place;
- Any data protection impact assessments you have carried out;
- A description of your data retention procedures, such as where data is stored, how long each category of data is kept, when data is deleted, and how deletion is verified;
- A description of what technical security measures you have taken;
- A description of your organisational security measures you have taken, including staff training and HR documentation; and

- a record of the policies you have put in place to deal with a data breach, including internal reporting mechanisms and contact structures.

DATA COLLECTION: KEY QUESTIONS TO ASK

1. Have you conducted an audit of the information you hold online?
2. Have you conducted an audit of the information you hold *offline*?
3. Have you conducted an audit of how information is retained, re-used, and shared?
4. Have you conducted an audit of what data you send *to* third parties?
5. Have you conducted an audit of what data you hold *from* third parties?
6. Have you reviewed the ways that your partners and third party suppliers audit, categorise, and inventory the data you share with them?

GDPR FOR ECOMMERCE - AREA 6: CONSENT AND LEGAL BASIS

Consent is one of the most misunderstood and misreported principles of GDPR. The new requirements are not as bad as the naysayers would have you believe. However, the new rules do indeed call for greater care and documentation from your business.

Under GDPR, *in most circumstances*, the data collection and processing you perform must be done with the **consent** of the people that data is about.

If consent is not the basis, your use of data must be **grounded in a legal justification**.

The consent mechanisms and legal bases you use to collect and process data must be clear, documented, and verifiable.

Your consent processes must be:

- **Active:** consent is freely given, specific, and unambiguous;
- Active consent must also be **positive**, meaning you have not presumed consent from a pre-ticked box, inactivity, or *not* selecting any option;
- Privacy must be presented as **granular** multiple choices, and not as a black-and-white, either-or dichotomy;
- **Unbundled:** users cannot be forced to grant consent for one thing in order to receive another;
- **Named:** the user must be made aware of all specific third parties who will be receiving their data and why they will be receiving it;
- **No imbalance in the relationship:** consent must not create an unfair relationship between the user and the data processor;
- **Verifiable and documented:** you must be able to prove who gave their consent, how consent was given, what information they were given, what they agreed to, when they consented, and whether or not the user has withdrawn their consent.

Your consent processes should include separate consent for advertising, tracking and marketing purposes. Users must be given the opportunity to actively opt in to the uses of their data for those purposes. They should no longer be bundled in as part of the basic service provision.

Likewise, users must be able to grant consent for the passing of their data to third parties for non-essential services. This, in GDPR parlance, means advertising, marketing, and profiling.

Regarding consent, your internal documentation must indicate:

- Who gave consent;
- How consent was given;
- What information they were given, and what they agreed to;
- When they consented (ideally a timestamped record); and
- Whether or not the user has withdrawn their consent.

As we discussed in the invocation of individual rights, users may withdraw their consent for any reason at any time, and they do not have to provide you with a reason for doing so.

Processing data without consent?

It is important to note there are circumstances outside of 'consent', where organisations may process customer data.

If the user relationship is **not** grounded in active consent, you **must** be able to justify your collection and processing of data in a **legal basis**, specifically that it meets one of the following requirements:

- A. Necessary for the performance of a contract;
- B. Necessary to comply with a legal obligation;
- C. Necessary to protect the person's vital interests (for example, providing emergency medical help);
- D. Necessary for the performance of a task in the public interest or in the exercise of official authority;
- E. Necessary for the purposes of the "**legitimate interests**" pursued by the controller or third party.

Item 'E' here, 'legitimate interests', is perhaps the most ambiguous, and most discussed, of these.

LEGITIMATE INTERESTS?

One of the more spoken about areas of GDPR in terms of processing data without consent is "Legitimate interests".

The UK's Information Commissioner explains this is best suited for situations where all of the following criteria apply:

- The processing is not required by law but is of a clear benefit to you or others;
- There's a limited privacy impact on the individual;
- The individual should reasonably expect you to use their data in that way; **and**
- You cannot, or do not want to, give the individual full upfront control (ie consent) or bother them with disruptive consent requests when they are unlikely to object to the processing.

Additionally, legitimate interest cannot be applied retroactively to any personal data already collected or processed.

The UK's Information Commissioner provides a useful chart, containing examples of which 'marketing methods' may likely be appropriately covered by 'legitimate interests', and which likely would not:

Marketing method	Is legitimate interests likely to be appropriate?
Post	✓
'Live' phone calls to TPS/CTPS registered numbers	X
'Live' phone calls to those who have objected to your calls	X
'Live' phone calls where there is no TPS/CTPS registration or objection	✓
Automated phone calls	X
Emails/text messages to individuals – obtained using 'soft opt-in'	✓
Emails/text messages to individuals – without 'soft opt-in'	X
Emails/text messages to business contacts	✓

SOFT OPT IN?

The table above is useful for ecommerce companies, as it illustrates that – at least in the United Kingdom – the body responsible for enforcing GDPR considers 'soft opt-in' (a method used by many online retailers to legally email existing customers) still an acceptable practice.

The UK's Information Commissioner further describes the practice of 'soft opt-in':

"The term 'soft opt-in' is sometimes used to describe the rule about existing customers. The idea is that if an individual bought something from you recently, gave you their details, and did not opt out of marketing messages, they are probably happy to receive marketing from you about similar products or services even if they haven't specifically consented. However, you must have given them a clear chance to opt out – both when you first collected their details, and in every message you send."

"The soft opt-in rule means you may be able to email or text your own customers, but it does not apply to prospective customers or new contacts (eg from bought-in lists). It also

does not apply to non-commercial promotions (eg charity fundraising or political campaigning).”

CONSENT & LEGAL BASIS: 8 KEY QUESTIONS TO ASK

1. Have you determined which aspects of your data collection and processing are grounded in consent, and which aspects are grounded in a legal basis?
2. Have you ensured that your consent processes meet the above criteria?
3. If not grounded in active consent, can you document and prove that your collection and processing of data is grounded in a legal basis?
4. Are you able to document proof of consent *or* legal basis for the data you collect and process?
5. Have you reviewed your existing consent mechanisms and records to ensure that your consent processes meet the above criteria?
6. If any aspect of the new criteria is missing, are you prepared to alter your consent mechanisms to refresh and secure GDPR-level consent?
7. If you are not able to re-establish consent under the GDPR requirements, does your data processing have a legal basis?
8. Are you prepared to cease data processing and delete records for cases where you cannot secure consent and have no legal basis?

GDPR FOR ECOMMERCE - AREA 7: ECOMMERCE BUSINESSES DEALING WITH CHILDREN

If your business targets children, or collects data from or about them, there are new requirements under GDPR that you will need to pay extra attention to in your sales processes.

This applies to the data you collect in the sales and fulfilment of goods orders as well as to the data created by children, for example, in apps and online games.

If your service targets children, there is a fascinating new requirement under GDPR: your must include a privacy notice written *for children in language that they can understand*. A child must understand what they are consenting to when they give their consent. Likewise, their adults must have a crystal clear understanding of the deeper uses of their data in the standard privacy notice which must also be included.

Expect the children of geeks everywhere to be roped into A/B testing for privacy policies.

DEALING WITH CHILDREN: 7 KEY QUESTIONS TO ASK

1. Are you aware whether or not you collect information about or from under-16s?
2. If so, have you documented the processes you use to protect this information?
3. Have you documented your additional data minimisation, storage, and deletion processes for under-16s' data?
4. Do children provide their information directly? If so, have you written a privacy notice for children in language they can understand?
5. Are you documenting evidence that you have parental consent for any data processing for under-16s?
6. Do you delete childrens' data records on request from a parent or guardian without requiring documentary evidence of the relationship?
7. Do you delete data that a child generated if that child is now an adult and requests that you do so?

GDPR FOR ECOMMERCE - AREA 8: DATA BREACHES

Data breaches can be disastrous for your customers and for your business as well. The truth of the matter, however, is that data breaches - whether caused by technical or by human factors - are almost always preventable.

GDPR requires you to do everything possible to prevent data breaches from happening, and also to prepare for data breaches in advance. You should audit your technical systems, as well as your human processes, for things that could open the door to a data breach happening.

Preparing for data breaches requires you to take an honest (and, possibly, quite uncomfortable) look at what aspects of your internal processes and cultures could contribute to a preventable breach. Any technology is only as good as the people behind it. Insecure staff are a far greater risk to data integrity than insecure databases.

In the event of a data breach, a data protection regulator can request documented evidence including the following:

- Details about the nature of a breach, such as what category of data was breached, how many individuals were affected, and how many data records were involved;
- Information on how you were alerted to a breach, and by whom;
- Any available information on who is responsible for a breach, or how it happened;
- What consequences are happening as a result of a breach;
- What measures you are taking to deal with a breach, such as contacting customers or resetting all passwords;
- What measures you are taking to deal with the consequences, such as unauthorised charges to customers' accounts;
- The name and contact details of your Data Protection Officer or the individual taking the lead on data breaches?

You should prepare a template in advance to collect and submit this information; the morning of a data breach discovery is not the time to find this out. High-risk breaches must be reported within 72 hours of discovery.

DATA BREACHES: 6 KEY QUESTIONS TO ASK

1. Do you regularly audit your systems and processes for potential data breach issues?
2. Do you know the criteria for a “high-risk”, reportable breach?
3. Have you created a template for GDPR’s data breach reporting requirements?
4. Have you conducted a postmortem of data breaches you may have experienced in the past?
5. Do you have an internal reporting mechanism in place to report potential data breaches before they happen?
6. Can staff report an issue, either technical or human, which could lead to a data breach, without fear of reprisal?

GDPR FOR ECOMMERCE - AREA 9: INTERNATIONAL AND PRIVACY SHIELD

Under European data protection law, personal data cannot be transferred outside of the EU to third countries unless that country ensures an 'equal and adequate' level of data protection.

Your ecommerce business must be prepared to:

- *Protect* your data at its origin and its destination, and
- *Provide* a legal means for that data to move.

To *protect* data, you must ensure that your non-EU partners and service providers have implemented a data protection system which is ***equal and adequate*** to GDPR for the European data you are sending them.

To *provide* a legal means, you must guarantee that your data is being transferred either under a framework agreement or through specific alternatives.

The major framework is Privacy Shield, which applies to US companies doing business with European data. Given the current political uncertainty, it is critical for you to ensure that your US-based partners and third party service providers are Privacy Shield compliant, ideally at the contract stage.

Alternatives to framework agreements include intra-company transfers and contractual clauses, all of which should be dealt with by a solicitor.

You must indicate in your privacy notices that data is being transferred outside the EU, and list all specific parties who receive that data as well as what they do with it. Your notices should also provide a means for users to object to their data being transferred outside the EU, keeping in mind that they need not provide a reason for asking you to do so.

If you work across European borders, your privacy notices must state your main country of establishment and your lead supervisory authority, in other words, the national data protection regulator who would handle concerns about your company.

INTERNATIONAL ISSUES: 6 KEY QUESTIONS TO ASK:

1. Are all of your partners and third party service providers in non-EU countries familiar with the new requirements under GDPR?
2. Are they already in compliance or is remedial work required?
3. Are your US-based partners and third party service providers Privacy Shield compliant?
4. Are you including and requiring GDPR compliance in your contracts with partners and service providers?
5. Are all international transfers of data, and the uses of that data, made clear in your public-facing privacy notices?
6. If you work across European borders, have you identified your main country of establishment and lead supervisory authority in your privacy notices?

GDPR FOR ECOMMERCE - AREA 10: "PRIVACY BY DESIGN" & "DATA PROTECTION BY DEFAULT"

GDPR requires designers, developers, and business owners to shift to a culture of **privacy by design** (Privacy by Design) and **data protection by default**.

This means that all your data-intensive processes, services, and applications must be designed with optimal privacy and data protection *built in from the start*.

This is in direct response to a culture which has encouraged minimal privacy and maximum sharing by default, with little or no consent possible from the user.

- Requiring logins via a social media account? Gone.
- Requiring microphone, body sensor, and contacts permissions to use an app? Gone.
- Requiring a user to consent to their web browsing data being passed to a coffee chain in order to use their loyalty app? Gone.

These changes are not before time, as far as many are concerned.

Key to the philosophy of data protection by default is a development framework known as Privacy by Design (Privacy by Design). This framework holds the following 7 principles:

1. Privacy must be **proactive**, not **reactive**, and must anticipate privacy issues before they reach the user. Privacy must also be **preventative**, not **remedial**.
2. Privacy must be the **default setting**. The user should not have to take actions to secure their privacy, and consent for data sharing should not be assumed.
3. Privacy must be **embedded into design**. Privacy is a core function of the product or service, not an add-on.
4. Privacy must be **positive sum** and should **avoid dichotomies**. For example, Privacy by Design sees an achievable balance between privacy and security, not a zero-sum game of privacy or security.

5. Privacy must offer **end-to-end lifecycle protection** of user data. This means engaging in proper data minimisation, retention, and deletion processes.
6. Privacy standards must be **visible, transparent, open, documented, and independently verifiable**.
7. Privacy must be **user-centric**. This means giving users granular privacy options, maximised privacy defaults, detailed privacy information notices, user-friendly options, and clear notification of changes.

Your Privacy by Design and Data Protection by Default obligations are internal, such as ensuring technical safeguards, making staff awareness of their legal obligations, and documenting best practices.

They are also external, such as publishing privacy notices, engaging in data minimisation and deletion, and providing users with granular privacy options.

One aspect of Privacy by Design is the creation of Privacy Impact Assessments (PIAs), which quite simply means a process by which the privacy risks inherent in a project are identified and addressed at the outset. Privacy by Design is the conversation you have with your team, your third party proviers, and your clients, before a single click's worth of work is done.

Ecommerce businesses should develop a Privacy Impact Assessment template for your data-intensive projects, and run a retrospective PIA on existing ones. The UK's Information Commissioner ICO has some [helpful guidance on the way forward](#).

PRIVACY BY DESIGN: 7 KEY QUESTIONS TO ASK

1. Have you reviewed your existing sites, apps, and processes for best Privacy by Design practice?
2. Have you reviewed your current points of data input for ways that data could be minimised? These could include "required" form fields, outdated marketing information, and customer records.
3. Have you developed a data retention and deletion policy for the different kinds of information you hold?

4. Have you reviewed the Privacy Impact Assessments of your partners and third party service providers?
5. Have you reviewed your process for verifying that data has been deleted?
6. Are you confident that you could share your Privacy by Design process with the general public?
7. Are you confident that your documented Privacy by Design process would pass muster with a regulator?

GDPR FOR ECOMMERCE - AREA 11: DATA PROTECTION OFFICERS

For organisations which engage in “large-scale” processing of personal data, which is likely to include many ecommerce businesses, the data protection officer - or Data Protection Officer - is a named individual who will carry legal and professional responsibility for data protection compliance.

DO YOU NEED A DATA PROTECTION OFFICER?

Do you need a Data Protection Officer? The UK’s Information Commissioner’s Office states:

Under the GDPR, you must appoint a DPO if:

- You are a public authority (except for courts acting in their judicial capacity);
- Your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); **or**
- Your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

For ecommerce companies, it’s less likely the first of these applies, also less likely the third applies (we discuss ‘special categories of data’ elsewhere), but the 2nd of these: “large scale, regular and systematic monitoring of individuals” may well apply, and indeed specifically mentions “online behaviour tracking”.

Two ambiguous areas within this are ‘core activities’, and ‘large scale, regular and systematic’. The Information Commissioner has provided further rough definitions of each:

WHAT ARE “CORE ACTIVITIES”?

“Your **core activities** are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (eg payroll or HR information), but which is not part of carrying out your primary objectives.”

WHAT IS ‘LARGE SCALE’, ‘REGULAR’, ‘SYSTEMATIC’?

“A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.”

THE ROLE OF A DPO

To use one somewhat misleading analogy, a Data Protection Officer is your health and safety officer for privacy and data protection. It is their job to be ever so slightly difficult:

“Why is that there?”

“Has that new hire been trained?”

“Wait a second: can we do that?”

“When was the last time we reviewed what’s in that storage room?”

Like the ever so slightly difficult health and safety officer, when the day comes, you will be grateful for their presence.

There are certain rights and protections a Data Protection Officer must have to do their job:

- They must be informed of all data protection issues in a transparent and timely matter.
- They must be made available to any user who has a concern over your use of their data
- They must maintain secrecy and confidentiality at all times with regards to personal data.
- They must be provided with all the resources necessary to do the job.
- ...and they must report directly to, and be in contact with, your highest level of management.

In addition, your Data Protection Officer cannot be told how to do their job, they cannot be punished or fired for raising questions you might rather not hear, and they cannot be given other tasks or responsibilities which could cause a conflict of interest.

A DPO's name and contact details must be publicly stated in your organisation's privacy notices. Their details must also be supplied to your data protection regulator, as they will be the first point of contact for concerns and queries.

DATA PROTECTION OFFICERS: 6 KEY QUESTIONS TO ASK

1. Have you determined *whether* you need a Data Protection Officer by law?
2. If not required, have you considered appointing a Data Protection Officer voluntarily?
3. Are you aware that a Data Protection Officer does not require any specific, formal, or legal qualifications?
4. While your Data Protection Officer can be part-time or contracted in, have you chosen a Data Protection Officer who is located within easy physical access of your premises?
5. Have you drawn up a list of what qualities would be desirable for a Data Protection Officer within the specific needs of your events business?
6. Are you prepared to give your Data Protection Officer a regular spot on your Board's agenda, if applicable?

SUMMARY

This guide is produced for the benefit of Ecommerce companies and readers interested in GDPR. All content was created by **Heather Burns** and **Dan Barker**.

- For enquiries about Digital Law and Tech Policy work, Heather is available at webdevlaw.uk
- For further information on Dan Barker, see barker.co.uk

For further information on Ecommerce Guide, visit us at EcommerceGuide.com or follow [@ecommerce](https://twitter.com/ecommerce).

If you have reached this point, and found any value in reading, please do share this guide with others. You can do so by sharing <https://ecommerceguide.com/guides/gdpr/> on Twitter, or LinkedIn, or via Email, or by reviewing the guide on Amazon at <https://bit.ly/ecommercegdpr>.

Disclaimer

This guidance pertains to EU data protection law through its implementation in the United Kingdom. The data protection authority in the UK, including Scotland, is the Information Commissioner's Office (ICO) at <https://www.ico.org.uk>.

All guidance and URLs provided in this document are current at the time of writing, but and are subject to change.

The information provided in this paper is not legal advice and its guidance is offered without prejudice.