



General Data Protection

Personal data protection becomes more and more important in the context of managing customer data and practices related to the management of an email marketing programme. The associated legal constraints tend to be more stringent and sanctions more dissuasive. In this context, the main expected development in Europe is driven by the new European regulation which will enter into enforcement on 25 May 2018. For most companies, this new regulation requires many changes to be made in advance before its entry into enforcement.

This document does not contain any legal advice for your company to use in complying with EU data privacy laws like the GDPR. Instead, it provides background information to help you better understand the GDPR. This legal information is not the same as legal advice, where an attorney applies the law to your specific circumstances, so we insist that you consult an attorney if you'd like advice on your interpretation of this information or its accuracy. In a nutshell, you may not rely on this as legal advice, or as a recommendation of any particular legal understanding.

We Know Email



returnpath.com

Table of Contents

Introduction to GDPR	4
What is the GDPR?	4
Who is concerned?	4
Personal data	4
How to Process Personal Data	5
Identify a lawful basis for legal processing	5
Additional information about those legal grounds.....	5
Process Flow for Selecting Legal Basis for Processing	6
Legitimate Interest.....	7
How legitimate interest might apply?	7
Example of when a controller may have a legitimate interest	7
Example of legitimate interest in action	7
The LIA—Legitimate Interests Assessment	7
The LIA is a 3 keys stages:	8
Specific rights for individuals for legitimate interest.....	8
Consent.....	9
The meaning of “consent”	9
Consent consideration	10
Current consent and re-permissioning	10
The Rights for Individuals.....	11
The right to be informed	11
The right of access	11
The right of rectification	11
The right to erasure (or the right to be forgotten)	12
The right restricts processing	12
The right to data portability	13
The right to object.....	13
Rights in relation to automated decision making and profiling	14
Implication and Sanction	15
Organisational implications.....	15
The sanction of the GDPR.....	15
Introduction to ePrivacy.....	16
What is the ePrivacy Regulation?.....	16
Main differences with GDPR	16
What does this law say?.....	16
What could be the implication for marketers?	17
Sources and Links for Further Information	18
World	18
France	18
UK.....	18
Local Authority	19
France	19



Germany	19
Spain	19
UK.....	19
Australia.....	20
Canada	20
Switzerland	20
Best Practice Examples	21
FAQ	26
How can I ensure I am formally compliant with the regulation?	27
How long does customer consent last?	27
Will I have to re-permission all the current contacts in my database?.....	27
Will Brexit affect GDPR?	27
Does “natural persons” apply to B2B?.....	28
Do I need to have consent to process or store personal data?	28
What does legitimate interest mean?	28
Are there any differences between B2B and B2C in GDPR, if so what are the major ones to look out for?	28
Does Switzerland have to be compliant with GDPR as they are not part of the EU?.....	28
Will GDPR affect my non-EU -based Business?	29



Introduction to GDPR

What is the GDPR?

The General Data Protection Regulation is the new European regulation on the processing of personal data. Its main objective will be to simplify and harmonise data protection in the 28 countries of the European Union. Fines will be applicable to companies in case of non-compliance.

The new act was adopted on April 2016 but will **come into force 25 May 2018**. In this context, all marketers will have to review their management rule and ensure that they don't violate the requirements.

Who is concerned?

This new regulation applies to all companies or organisations located within an EU Member State but also outside the EU as long as they collect, process or store personal data from EU citizens. If a company works with data processors it must ensure that it will be able to comply with the GDPR.

Personal data

“Any information relating to an identified or identifiable natural person: an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.”



How to Process Personal Data

Identify a lawful basis for legal processing

The controllers will have to identify a lawful basis for processing personal data and document it. They will need one of the six following legal grounds:

- **Consent:** is an objective legal ground. The controller will have to ask the individuals for consent before processing their personal data.
- **Contractual:** the controller may need personal data for the performance of a contract. For example, the name and the address are required to deliver a purchase, and the controller needs to share that information to a delivery company.
- **Legal obligation:** the controller may need to process Personal Data to be compliant with a legal obligation. For example, in the financial sector it could be for fraud prevention.
- **Vital Interests:** in other words to protect the data subject's rights. For example, the transfer of health record from a GP surgery to the hospital where the data subject is currently being treated.
- **Public task:** the controller may need to process Personal Data for the performance of a task carried out in the public interest or in the exercise of official authority. For example, the controller will have to share the salary details from the employee to HM revenue and customs to calculate income tax coding.
- **Legitimate interest (LI):** is a subjective legal option. The controller needs to process Personal Data for the purpose of the Legitimate Interests.



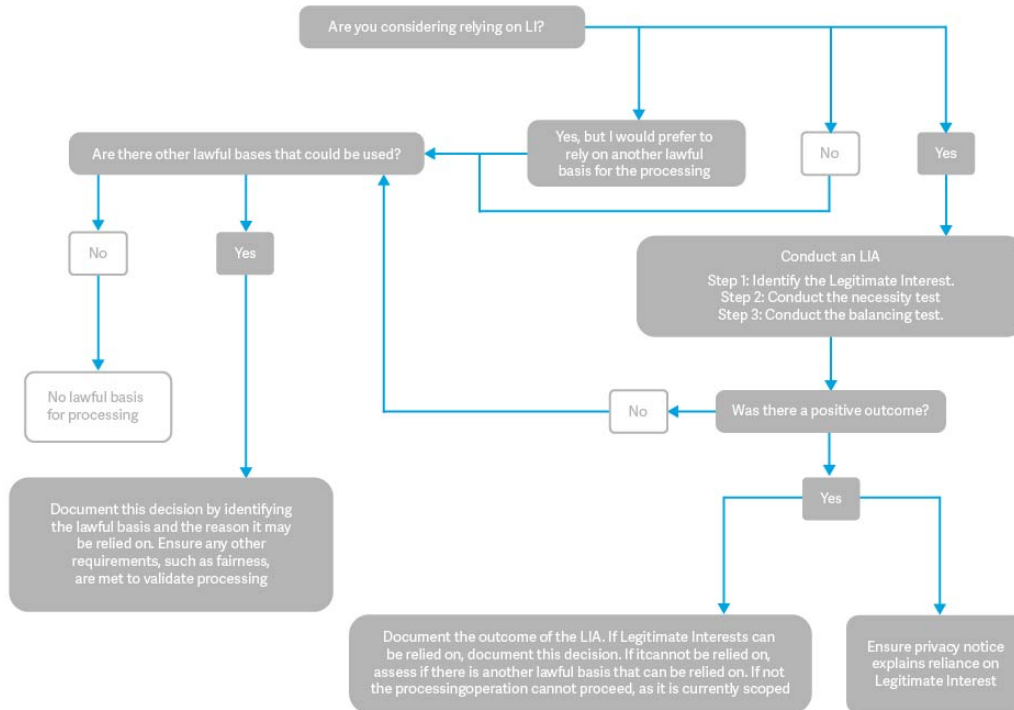
See the infographic from the DMA which introduces you to each legal ground: [DMA insight: Six legal bases of processing data](#).

Additional information about those legal grounds

- **There is no hierarchy** of lawful grounds for processing Personal Data. All are equally valid. There is different lawful basis for different processing. The most appropriate ground will depend on the Personal Data being processed and the purposes of processing.
- **Each legal ground may have different privacy rights of individuals.** There are different rules between LI and Consent. If the controller relies on LI for processing Personal Data, the individual has the right to object to profiling. But if the controller relies on consent the individual does not have this right (although he can withdraw his consent at any time).

Process Flow for Selecting Legal Basis for Processing

Potential Personal Data Processing Operation Identified



Most of the email marketing sender will be concerned by the legal grounds:

- [Legitimate interest \(LI\)](#)
- [Consent](#)



Legitimate Interest

How legitimate interest might apply?

- **Three stage test:** the controller has to pass this [three stage test](#).
 1. Identify a legitimate interest
 2. Carry out a necessity test
 3. Carry out a balancing test
- **Relationship:** the nature of the relationship should be weighed against the necessity of the processing and the impact on the individual. This is a key element.
- **Third parties:** a direct relationship is not essential for relying on LI but the controller will have to inform individuals how they obtained the personal data.

Example of when a controller may have a legitimate interest

Here are three specific examples that may be pertinent for marketers:

- **Direct marketing:** the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest (recital 47).
- **Reasonable expectation:** individuals have a reasonable expectation that their data will be used.
- **Relationship and appropriate relationship:** relevant and appropriate relationship in a situation where the individual is a client.

Example of legitimate interest in action

- **Suppression:** you may have to hold personal data to ensure no more direct marketing is sent to the individual.
- **Personalisation:** you enhance and personalise the user experience you offer to your customers.
- **Web analytics:** you use diagnostic analytics to access the number of visitors, posts, pageviews, reviews and followers in order to optimise future marketing campaigns.
- **Direct marketing:** a charity sends a postal mailshot out to existing supporters providing an update on its activities and details of upcoming events.
- **Artificial Intelligence:** your customer service department is putting in place algorithms that help to manage customer service requests.

The LIA—Legitimate Interests Assessment

The LIA is advisable for the controller in order to:

- ensure compliance
- maintain a written record that it has carried out an LIA
- maintain the reasons why it came to the conclusion that it met the balancing test elements



These LIAs may be disclosed to other controllers in the event of a sale or acquisition of personal data, where legitimate interests is the lawful basis of processing, as part of the due diligence process. The controller to whom personal data is disclosed will need to review the LIAs and update them where processing activities will differ. Additional requirements set out in the GDPR may also need to be met, such as notification of changes to processing.

The LIA is a 3 keys stages:

- 1. Identify a legitimate interest:** What is the purpose for processing the personal data and why is it important to the controller or to a third party? The LIA will only cover relevant processing of the controller and the disclosure of the personal data. Third party would have to conduct their own LIA.
- 2. Carry out a necessity test:** The controller will have to consider whether the processing of personal data is “necessary.” Necessary doesn’t mean “indispensable.” It may be easier to ask: “Is there another way of achieving the identified interest?”
- 3. Carry out a balancing test:** The controller will have to evaluate the rights and freedoms of the individual. The balancing test must always be conducted fairly. The balancing test needs to response those questions:
 - Would or should the individual expect the processing to take place?
 - What type of data are you processing? (be careful with data relating to a child)
 - What is the impact on the individual? (positive or negative)

Specific rights for individuals for legitimate interest

Overall the GDPR provides [rights for individuals](#), many of which apply whatever the basis of processing, although there are some exceptions:

- **The right to be informed:** the individual must be told about those LI and about their right to object.
- **Right to erasure:** this is not an automatic right when data are processed for LI (would be the case for consent). This applies if you can’t justify the legitimacy of the processing.
- **The right to object:** the individual must be told about the LI and can be highlighted at the point of data collection and in a section of the privacy notice. Guidance from the DMA said that for direct marketing, the controller should consider an unsubscribe link or online preference centre.
- **The right of data portability:** this right does not extend to personal data processed with the LI. All of this will be explained in more detail later in the reading.



See the complete guidance from the Data Protection Network in collaboration with the DMA: [Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation](#).

Consent

The meaning of “consent”

- **Unbundled**—Consent must be separate from other terms and conditions. It can't be a condition to sign-up to any service.
- **Active**—There must be some form of clear affirmative action (in other words: a positive opt-in). Silence, pre-ticked boxes or inactivity can't constitute consent.
 - Examples of active opt-in mechanisms include:
 - Signing a consent statement on a paper form
 - Ticking an opt-in box on paper or electronically
 - Clicking an opt-in button or link online
 - Selecting from equally prominent yes/no options
 - Choosing technical settings or preference dashboard settings
 - Responding to an email requesting consent
 - Answering yes to a clear oral consent request
 - Volunteering optional information for a specific purpose—e.g., filling optional fields in a form (combined with just-in-time notices) or dropping a business card into a box
- **Granular**—Consent for different types of processing (wherever appropriate) should be separate.
- **Named**—Name of the organisation or third parties who will be relying on consent should be specified.
- **Documented / Verifiable**—Consent of the subscriber must be provable at any time. It is essential that the data controller keep track of:
 - **Who consented:** the name of the individual or other identifier (e.g., online user name, session ID).
 - **When they consented:** a copy of a dated document, or online records that include a timestamp; or, for oral consent, a note of the time and date which was made at the time of the conversation
 - **What they were told at the time:** a master copy of the document or data capture form containing the consent statement in use at that time, along with any separate privacy policy, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time
 - **How they consented:** for written consent, a copy of the relevant document or data capture form. If consent was given online, your records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, you should keep a note of this made at the time of the conversation—it doesn't need to be a full record of the conversation
 - **Whether they have withdrawn consent:** and if so, when.
- **Easy to withdraw**—The natural person has to be informed that they have the right to withdraw their consent at any time, and how to do this. The mechanism to withdraw has to be simple and effective.



- **Parental consent**—Parental consent will be required for young persons in the EU under 16 years. The age derogate to the country. In the UK the government believes 13 is most appropriate.

Consent consideration

- If you are using **special category data**, you are more likely to need to seek explicit consent to legitimise the processing, unless one of the other specific conditions in Article 9(2) applies.
- You are also likely to need consent under **ePrivacy laws** for most marketing calls or messages, website cookies or other online tracking methods, or to install apps or other software on people's devices.
- These rules are currently found in the **Privacy and Electronic Communications Regulations 2003 (PECR)**, but there is a proposal for a new updated **ePrivacy Regulation** to come into force at the same time as the GDPR. The Regulation has not yet been finalised.

Current consent and re-permissioning

Existing customers may not have the correct permissions for receiving communications from your organisation.

If you rely on individuals' consent to process their data, **make sure it will meet the GDPR standard on being specific, granular, clear, and prominent, opt-in, properly documented and easily withdrawn**. In that case, you will be able to rely on that consent post-GDPR.

If the consent you obtain pre-GDPR is ambiguous and don't meet the GDPR standard for consent this suggests that companies may need to gain opt-in consent from existing customers by implementing repermissioning strategies.

However, the regulation does indicate that organisations can continue to lawfully process personal data from their existing database **if they can demonstrate "legitimate interest."** In Article 47 of the GDPR, it states that the processing of personal data for direct marketing purposes may be regarded as a legitimate interest.



The Rights for Individuals

Overall the GDPR provides the following rights for individuals, many of which apply whatever the basis of processing:

The right to be informed

At the point of collection of the data: processing information has to be provided, typically through a privacy notice.

- It emphasises the need for transparency over how you use personal data.
- The information you supply is determined by whether you obtained the personal data directly from individuals.
- Much of the information you should supply is consistent with your current obligations under the Data Protection Act, but there is some further information you are explicitly required to provide. The information you supply about the processing of personal data must be:
 - Concise, transparent, intelligible and easily accessible;
 - Written in clear and plain language, particularly if addressed to a child; and free of charge.

Here is a [link to a privacy notice checklist](#) provided by the ICO with all the information to be supplied.

The right of access

The individuals will have the right to obtain for free:

- Confirmation that their data is being processed
- All the personal data stored on them
- All the information provided in the privacy notice (see point 1. above)

These are similar to existing subject access rights under the Data Protection Act.

You must verify the identity of the person making the request, using “reasonable means.”

If the request is made electronically, you should provide the information in a commonly used electronic format.

You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at the latest within one month of receipt.

You will be able to extend the period of compliance by a further two months when requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

The right of rectification

The natural person can ask the organisation to rectify their personal data if it finds any inaccuracies.



- Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.
- You must respond within 30 days. This can be extended by 60 days (for a total of 90 days) where the request for rectification is complex.
- Where you are not taking action in response to a request for rectification, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure (or the right to be forgotten)

It authorises any person to request the erasure of data concerning him.

- This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- The right to erasure does not provide an absolute “right to be forgotten”. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. There are some specific circumstances where the right to erasure does not apply and you can refuse to process a request. In that case, the data processor must explain the reason why the individual’s data are kept.
- Under the Data Protection Act, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this threshold is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

When a request for erasure is made and the organisation has shared this data with third-party processors, the organisation needs to do everything it can to inform the third party processor of the erasure.

The right restricts processing

Individuals have a right to “block” or suppress processing of personal data. When processing is restricted, the storage is still permitted.

- Under the Data Protection Act, individuals have a right to “block” or suppress processing of personal data. The restriction of processing under the GDPR is similar.
- When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future.
- You will be required to restrict the processing of personal data in specific circumstances.
- You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.



- If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- You must inform individuals when you decide to lift a restriction on processing.

The right to data portability

- The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- The right to data portability only applies:
 - to personal data an individual has provided to a controller;
 - where the processing is based on the individual's consent or for the performance of a contract; and
 - when processing is carried out by automated means.

The right to object

If the processing is based on legitimate interests or the performance of a task in the public interest/exercise of official authority.

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

If you process personal data for direct marketing purposes

- You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- You must deal with an objection to processing for direct marketing at any time and free of charge.
- You must inform individuals of their right to object “at the point of first communication” and in your privacy policy.

This must be “explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.”



Rights in relation to automated decision making and profiling

The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular, to analyse or predict their: performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements. When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place. The controller must ensure that individuals are able to:

- Obtain human intervention
- Express their point of view
- Obtain an explanation of the decision and challenge it



Implication and Sanction

Organisational implications

From 25 May, any company, responsible for data processing will have to:

- Verify its possible obligation to designate a Data Protection Officer (DPO)
- Set up a "register of processing activities"
- Take technical measures of encryption and "pseudonymisation" of the processed data
- Ensure transparency, which means the right information about the right of the people whose data is processed

The sanction of the GDPR

The GDPR provides for graduated financial penalties which may be very substantial for infringing companies.

The most serious breaches will incur a fine of up to four percent of the company's overall turnover. This will especially concern breaches of the fundamental principles of the law in particular the respect for privacy.

A fine of up to two percent of the company's overall turnover can be applied if the company doesn't track all relevant information or fails to notify the authority and the concerned persons of the detection of an infringement of personal data.

The breach of the obligation to notify is considered as a serious violation of the legislation and will be severely punished.



Introduction to ePrivacy

What is the ePrivacy Regulation?

The European Union ePrivacy Regulation has been published to broaden the scope of the current ePrivacy Directive and align the various online privacy rules that exist across EU member states. The regulation takes on board all definitions of privacy and data that were introduced within the General Data Protection Regulations, and acts to clarify and enhance it.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards to traffic and location data, itemised billing, line identification, and directory listings.

Main differences with GDPR

Each regulation was drawn up to reflect a different segment of EU law. The GDPR was created to enshrine Article 8 of the European Charter of Human Rights in terms of protecting personal data, while the ePrivacy regulation was created to enshrine Article 7 of the charter in respect to a person's private life. The private sphere of the end user is covered under the ePrivacy regulations, making it a requirement for a user's privacy to be protected at every stage of every online interaction.

It is important to remember that the ePrivacy regulation was created to complement and particularise the GDPR, so the rules of the GDPR are always relevant and an overall part of the legislative aspects of the ePrivacy.

The ePrivacy directive takes the broad online retail sector into account in terms of how personal information might be used and in this sense is what it adds to the overall regulations that make up the GDPR.

What does this law say?

The current proposal is under negotiation in Europe and it is possible that some text may change. However, GDPR is law, so any changes made should not contradict the GDPR or its principles. The proposal should be approved in May 2018.



What could be the implication for marketers?

This regulation is likely to impact B2B marketing. In line with the GDPR's wider scope of personal data, data relating to someone at their place of business is that person's personal data. This is reflected in the new directive, where there is no distinction between B2B and B2C personal data. If we put that in the context of B2B email marketing, whereas before you could email someone as long as you gave them the opportunity to opt out, now the rules are the same as B2C.

This means that you need to use either consent, or the so-called "soft opt in" principle. Both the Article 29 working party and the European Data Protection Supervisor have asked that the regulation makes this treatment of B2B personal data clear. The idea that a right can be given to you by one hand with the GDPR and taken away with the other under the e-Privacy regulation is counterintuitive.



Sources and Links for Further Information

Here is a selection of links to get more information about this new law:

World

- The full GDPR text: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

France

- Règlement européen sur la protection des données : ce qui change pour les professionnels: <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>
- Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016: <http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR>

UK

- The ICO's Data Protection Reform website: <https://ico.org.uk/for-organisations/data-protection-reform/>
- The ICO's GDPR overview: <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>
- The DMA's (Direct Marketing Association) helpful information: <https://dma.org.uk/gdpr>
- The Data Protection Network's GDPR Legitimate Interests guidance: https://dma.org.uk/uploads/misc/59ca0f2e17ef3-dpn-li-guidance-publication_59ca0f2e17e5a.pdf
- The ICO's GDPR Consent Guidance: <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>
- B2B Marketing blog post by Guy Hanson - GDPR and email: The heart of the new data protection regulation: <https://www.b2bmarketing.net/en-gb/resources/blog/gdpr-and-email-heart-new-data-protection-regulation>

Local Authority

UNDER GDPR

France

- **CNIL**: The Commission Nationale de l'Information et des Libertés is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data. <https://www.cnil.fr/>

Germany

- **BfDI**: The Federal Commissioner for Data Protection and Freedom of Information (BfDI) is the federal commissioner not only for data protection but also, since the commencement of the German Freedom of Information Act on January 1, 2006, for freedom of information. Since 2016, it has been an independent federal agency, in accordance with EU regulations. https://www.bfdi.bund.de/DE/Home/home_node.html

Spain

- **AEPD** (Agencia Española de Protección de Datos): The Spanish Data Protection Agency is an agency of the government of Spain. <https://www.agpd.es/portalwebAGPD/index-ides-idphp.php>

UK

- **ICO**: The Information Commissioner's Office is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport (DCMS). It is the independent regulatory office (national data protection authority) dealing with the Data Protection. <https://ico.org.uk/>



UNDER ANOTHER REGULATION

Australia

- **OAIC:** The Office of the Australian Information Commissioner is an independent Australian Government agency, acting as the national data protection authority for Australia, established under the Australian Information Commissioner Act 2010. <https://www.oaic.gov.au/>

Canada

- **OPC:** The Privacy Commissioner of Canada is an Agent of Parliament whose mission is to protect and promote privacy rights. The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's federal private-sector privacy law. <https://www.priv.gc.ca/en>

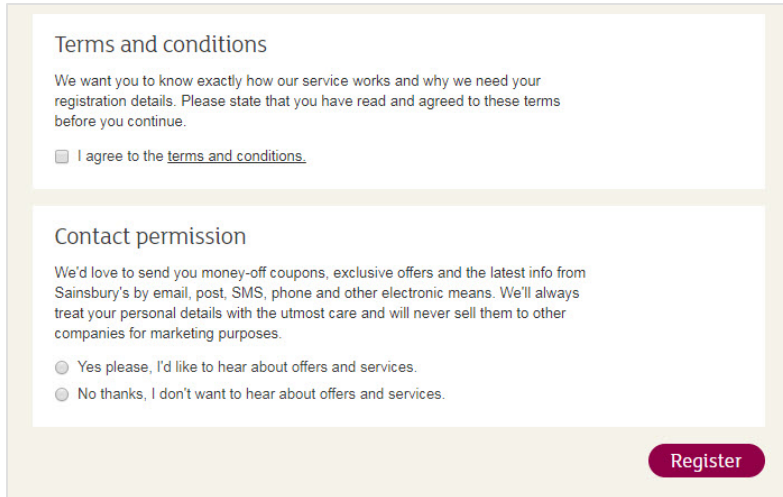
Switzerland

- **FDPIIC:** The Federal Data Protection and Information Commissioner (FDPIIC) is responsible to advise, educate and ensure the protection of personal data in Switzerland. It is established by the Federal Act on Data Protection[3] and by the Federal Act on Freedom of Information in the Administration. <https://www.edoeb.admin.ch/index.html>



Best Practice Examples

Asking for Consent – Unbundled and active – Sainsbury’s



Terms and conditions

We want you to know exactly how our service works and why we need your registration details. Please state that you have read and agreed to these terms before you continue.

I agree to the [terms and conditions](#).

Contact permission

We'd love to send you money-off coupons, exclusive offers and the latest info from Sainsbury's by email, post, SMS, phone and other electronic means. We'll always treat your personal details with the utmost care and will never sell them to other companies for marketing purposes.

Yes please, I'd like to hear about offers and services.
 No thanks, I don't want to hear about offers and services.

Register

Unbundled: Sainsbury’s separate “Terms and conditions” and “Contact permission” section thanks white content block.

Active: Sainsbury’s is using a radio button to choose either “Yes, please” or “No, thanks”.

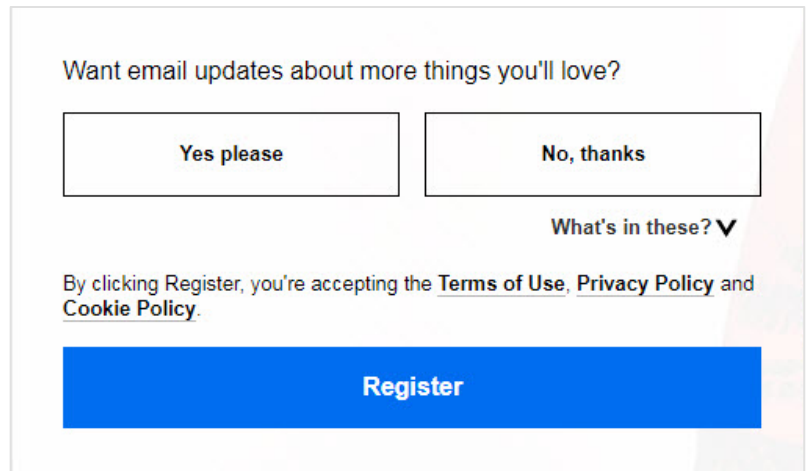
Improvement to be made: Sainsbury’s is asking permission for email, post, SMS, and telephone with the same radio button. It is not granular. All channels should have their own checkbox/radio buttons.

Asking for Consent – Affirmative – BBC

Affirmative:

In the BBC account sign up process, users are asked if they would like to receive email updates.

Two options are given – yes or no. One must be chosen.



Want email updates about more things you'll love?

What's in these? ▼

By clicking Register, you're accepting the [Terms of Use](#), [Privacy Policy](#) and [Cookie Policy](#).

Register

Asking for Consent – Granular – Cancer Research UK

Join us

Become part of the movement to bring forward the day when all cancers are cured. Hear about our latest breakthroughs, campaigns and how you can help support our life-saving work.

Email Yes No

Text message Yes No

Post Yes No

Phone Yes No

Your details are safe with us. We will never share them with anyone else. By pressing 'Complete my donation' I confirm that the above details are correct and that I have read and agreed to Cancer Research UK's [terms and conditions](#) and [privacy statement](#).

Complete my donation

Granular: Cancer Research UK uses four different checkboxes: Email, Text message, Post, Phone.

Asking for Consent – Named – Waitrose

Named: Waitrose has a checkbox for receiving consent for each organisation (Waitrose, John Lewis, and John Lewis Financial Services).

Improvement to be made: Those checkboxes are opt-out. It means the user has to check the boxes if he doesn't want to receive communications. It is not an active consent.

At Waitrose, we have exciting offers and news about our products and services that we hope you'd like to hear about. By providing your details you agree to be contacted by us*. We will treat your data with respect and you can find the details in our [Contact Promise](#).

If you would prefer not to hear from us, you can stop receiving our updates at any time by getting in touch or by letting us know below.

I'd prefer **not** to receive updates from Waitrose

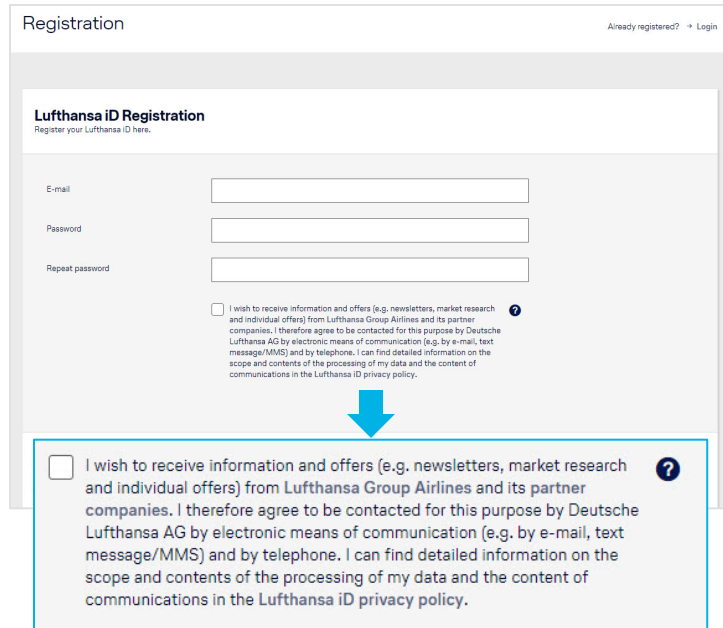
I'd prefer **not** to receive updates from John Lewis

I'd prefer **not** to receive updates from John Lewis Financial Services

If you have a my John Lewis membership card, we'll be unable to continue your **my John Lewis** membership if you opt out of receiving information from John Lewis itself.



Asking for Consent – Active – Lufthansa



The screenshot shows the 'Lufthansa iD Registration' form. It includes fields for E-mail, Password, and Repeat password. Below these fields is a checkbox for consent:
 I wish to receive information and offers (e.g. newsletters, market research and individual offers) from Lufthansa Group Airlines and its partner companies. I therefore agree to be contacted for this purpose by Deutsche Lufthansa AG by electronic means of communication (e.g. by e-mail, text message/MMS) and by telephone. I can find detailed information on the scope and contents of the processing of my data and the content of communications in the Lufthansa iD privacy policy.
 A blue arrow points from this checkbox to a larger, highlighted version of the same checkbox and text below.

Active: Lufthansa has a checkbox for their email programme subscription.

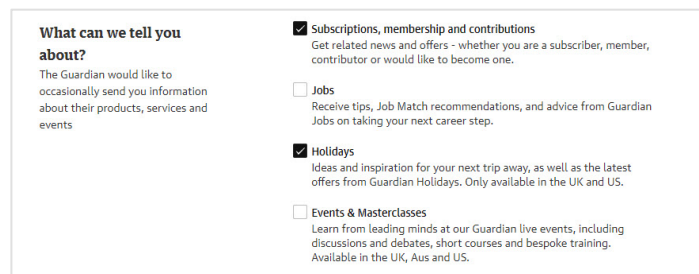
We can see that the subscription is optional.

Clear: The description of the checkbox is very clear and exhaustive about the email programme.

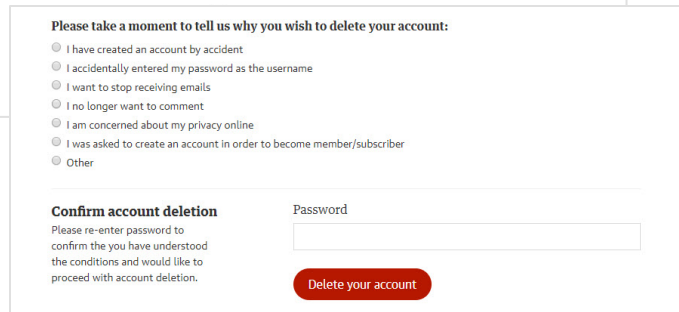
Consent – Easy to Withdraw – The Guardian

Easy to Withdraw: The Guardian provides in the subscriber's account the possibility to withdraw the permission for profiling and for sending emails. The subscribers only have to uncheck the box.

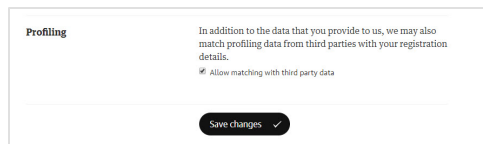
Account Deletion: The Guardian provides the subscribers the possibility to delete their account as well.



The screenshot shows account settings for 'What can we tell you about?'. It lists several categories with checkboxes:
 Subscriptions, membership and contributions: Get related news and offers - whether you are a subscriber, member, contributor or would like to become one.
 Jobs: Receive tips, Job Match recommendations, and advice from Guardian Jobs on taking your next career step.
 Holidays: Ideas and inspiration for your next trip away, as well as the latest offers from Guardian Holidays. Only available in the UK and US.
 Events & Masterclasses: Learn from leading minds at our Guardian live events, including discussions and debates, short courses and bespoke training. Available in the UK, Aus and US.



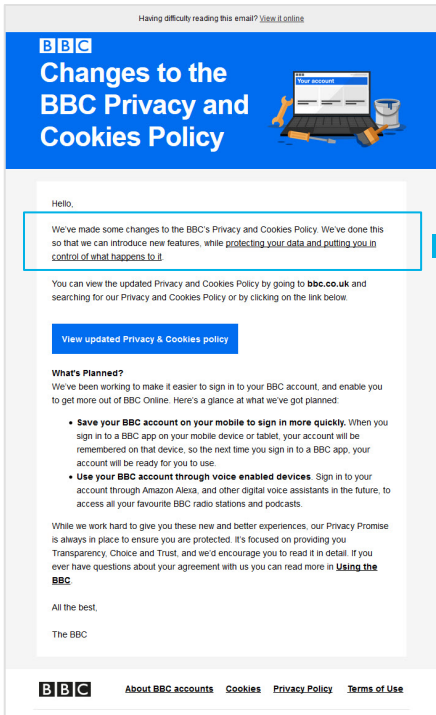
The screenshot shows the account deletion process. It starts with a question: 'Please take a moment to tell us why you wish to delete your account:'. Below are radio button options:
 I have created an account by accident
 I accidentally entered my password as the username
 I want to stop receiving emails
 I no longer want to comment
 I am concerned about my privacy online
 I was asked to create an account in order to become member/subscriber
 Other
 Below this is a 'Confirm account deletion' section with a password field and a 'Delete your account' button.



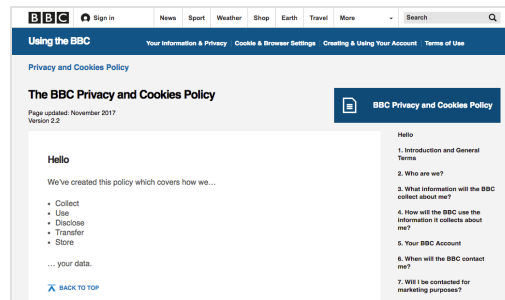
The screenshot shows the 'Profiling' settings. It states: 'In addition to the data that you provide to us, we may also match profiling data from third parties with your registration details.' There is a checkbox for 'Allow matching with third party data' which is checked. A 'Save changes' button is at the bottom.



Email – Privacy Policy Changes – BBC

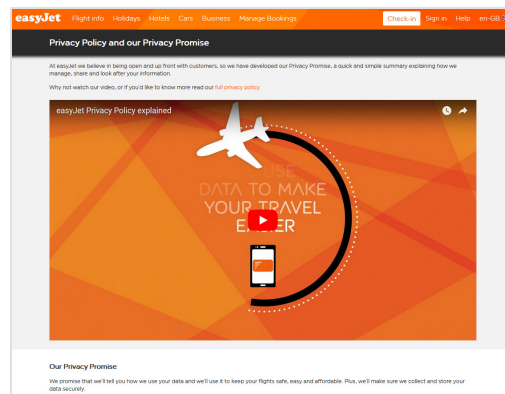
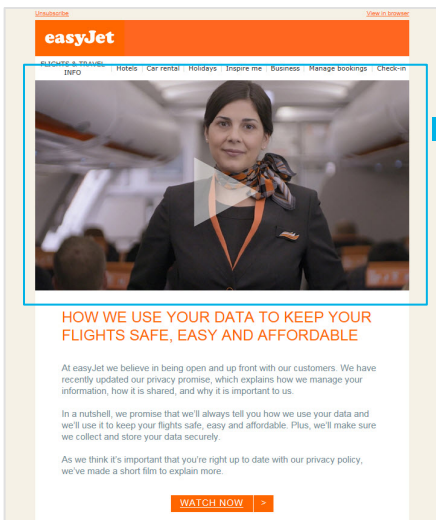


Link to a privacy promise



Link to the full version of the Privacy Policy

Email – Privacy Policy Changes – easyJet



Link to a video explaining the privacy policy promise

Communication – Re-permissioning – Manchester United

The law is changing, to continue to receive emails from Manchester United you **MUST** complete this form. Enter your details before 31st December for the chance to win 1 of 10 signed shirts.

STAYUNITED

Title Please select

Name*
First Name _____ Last Name _____

Email Address*
me@email.com

Mobile _____

Date of Birth*
Day _____ Month _____ Year _____

Country*
Please select a country

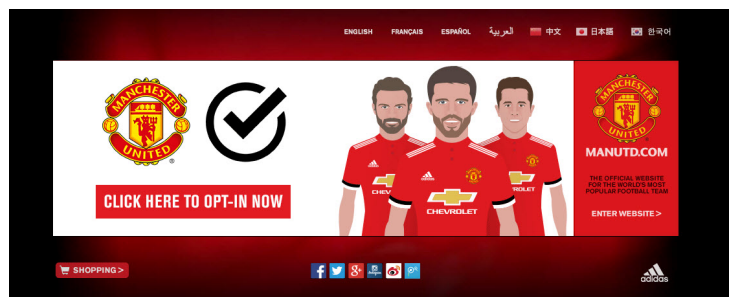
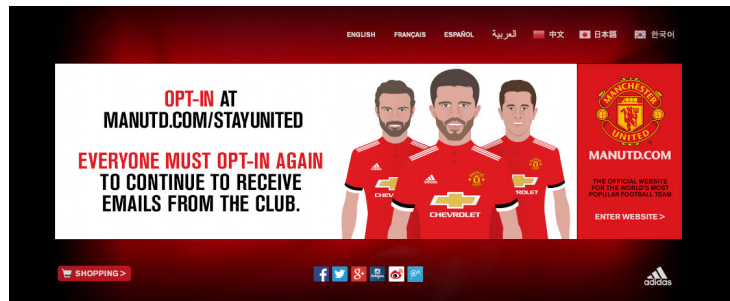
We want you to be first to know about New Signings, Competitions, Club News, Ticket Availability and occasional offers from **official sponsors and partners**. To stay updated, select YES:

Yes
 No

You can change your preferences or unsubscribe at any time in your Preference Centre. By signing up, you agree to Manchester United Limited's (M.U.L.) use of your personal data in accordance with our Privacy Policy. We use your data to personalise and improve your experience on our digital platforms, provide products and services you request from us, and carry out profiling and market research. Please read the competition Terms & Conditions for further details.

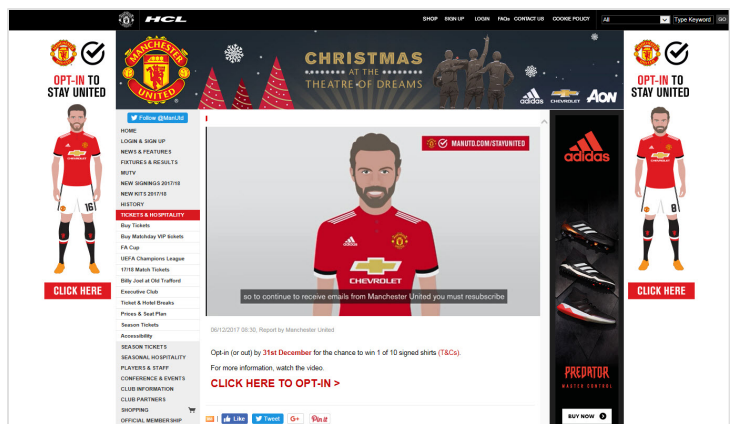
SUBMIT

OPT-IN (OR OUT) BY 31ST DECEMBER FOR THE CHANCE TO WIN ONE OF TEN SIGNED SHIRTS



On the homepage of the website, they ask to opt-in again. They also ran a promotion to win a signed shirt if opt-in before 31st of December.

Banners on each page of the website “to stay united.” They also featured a video explaining that subscribers need to opt-in again.



FAQ

- [How can I ensure that I am formally compliant with the regulation?](#)
- [How long does customer consent last?](#)
- [Will I have to re-permission all the contact in my database?](#)
- [Will Brexit affect GDPR?](#)
- [Does “natural persons” apply to B2B?](#)
- [Do you need to have consent to process or store personal data?](#)
- [What does legitimate interest mean?](#)
- [Are there any differences between B2B and B2C in GDPR, if so what are the major ones to look out for?](#)
- [Does Switzerland have to be compliant with GDPR as they are not part of the EU?](#)
- [Will GDPR affect my non-EU -based Business?](#)



How can I ensure I am formally compliant with the regulation?

By following our recommendations you should meet the majority of the requirements. To be formal about the deployed practices, we invite you to contact a specialised lawyer.

How long does customer consent last?

The law says that consent is given “for the time being”, but with the ICO adding that “consent decays over time” what is the lifespan of consent? Unfortunately, this is where the laws and guidance become less specific. The ICO has made a recommendation for third party data that consent should be considered invalid after six months. In essence, this means that marketers would have six months from the initial collection for first use. On the topics of postal and all first-party marketing data, however, there are no time frames offered in the ICO’s guidance to date.

Will I have to re-permission all the current contacts in my database?

If you feel that your current permissioning does not meet the new GDPR regulations (e.g. implied consent) consider running a re-permissioning campaign. This would involve an email, or a series of emails, designed to encourage the recipient to take an action to confirm that they would still like to receive emails from you.

Consider adding this process in your strategy in multiple ways:

- As a standard part of all emails sent to the user between now and May.
- As part of a preference centre launch campaign encouraging them to provide more information to make their email communications more relevant.
- As a standalone campaign to seek final permission before removal.

Standalone campaign:

- This is a series of emails telling the subscriber that you will stop sending them emails if they do not click the specific link in the email to confirm they would like to stay on your list and continue to receive messages from you.
- Once a re-permissioning series has been sent, and you don’t get confirmation that they want to stay on your email list, remove these subscribers from your list.

Here is a very interesting article on [this topic](#).

Will Brexit affect GDPR?

No, Brexit won’t affect GDPR. UK was bound to the GDPR before the decision to leave the EU and will mirror GDPR and the updates to ensure continued data-sharing with the rest of the EU post-Brexit.



Does “natural persons” apply to B2B?

While companies are not “natural persons”, individuals who work at those companies are, so the GDPR will apply equally to consumer and business-to-business data.

Do I need to have consent to process or store personal data?

No, you don’t necessarily need consent to process or store personal data if you are able to prove that you have a legitimate interest (see below for the meaning of “[Legitimate Interest](#)”).

What does legitimate interest mean?

The ICO (Information Commissioner’s Office) called for the industry to work with regulators to make sure it has the guidance it needs and the DPN (Data Protection Network) answered the call. In collaboration with DMA’s members, they produced practical guidance for marketers on legitimate interests. [Here is the guidance.](#)

Are there any differences between B2B and B2C in GDPR, if so what are the major ones to look out for?

The GDPR applies to personal data. Most B2C and B2B data used in direct marketing are personal data and so the GDPR applies.

The ePrivacy Regulation due to be introduced on 25 May 2018 has specific rules for B2C and B2B marketing. A lobbying focus for the DMA.

Does Switzerland have to be compliant with GDPR as they are not part of the EU?

The current Swiss Data Protection Act (DPA) is twenty-five years old and a brand new law is being prepared by our federal authorities. It is not expected to enter into force before 2019.

Even though the new regulation comes from the EU, it does impact organisations in Switzerland. If you answer “yes” to any of the following questions, GDPR does apply to your organisation and the data you hold about European individuals.

- Does your organisation offer services or goods to individuals in the EU?
- Does your organisation process or participate in the processing of personal data of EU individuals, for itself or on behalf of another organisation?
- Does your organisation monitor online behaviour of users based in the EU?
- Does your organisation analyse the activities of EU users when they are using your organisation’s app or browsing its website?



Will GDPR affect my non-EU -based Business?

Article 3 of the GDPR says that if you collect personal data or behavioural information from someone in an EU country, your company is subject to the requirements of the GDPR.

Two points of clarification:

- First, the law only applies if the data subjects, as the GDPR refers to consumers, are in the EU when the data is collected. This makes sense: EU laws apply in the EU. For EU citizens outside the EU when the data is collected, the GDPR would not apply.
- The second point is that a financial transaction doesn't have to take place for the extended scope of the law to kick in. If the organisation just collects “personal data”—EU-speak for what we in the U.S. call personally identifiable information (PII)—as part of a marketing survey, then the data would have to be protected GDPR-style.

