GDPR Checklist

Introduction:

The new General Data Protection Regulation (GDPR) determines how your business does business from May 2018.

There are big changes on the way. Your business will need to manage, administer and protect personal data whether you work in B2B or B2C marketing.

To help you prepare we have developed this GDPR checklist based on the latest information available. Use it to assess your business and find out which areas you need to focus on.

While this checklist is as up-to-date as possible, guidance may change right up to May 2018.

Find the latest version:

dma.org.uk/article/dma-advice-gdpr-checklist

1 Legitimate interests

- [ ] We check that legitimate interests is the most appropriate lawful basis for processing
- [ ] We explain how or why we need an individual's personal data when we collect it
- [ ] We use a layered privacy notice/policy

  A layered privacy notice puts the most important information upfront and then there is a more detailed privacy policy underneath it
- [ ] Individuals are well informed of what we plan to do with their data when we collect it
- [ ] We give individuals the option to refuse marketing

  This right is explicitly stated and it's easy to exercise that right
- [ ] We collect the minimum data necessary and delete records after use

  We can keep data needed for a suppression file

  We need a valid reason to process an individual's personal data using your legal legitimate interests. Direct marketing is recognised as a legitimate interest in GDPR recital 47.

  For example, an individual may have bought a product from a business so that business can market similar products to the customer

Whether you rely on consent or legitimate interests for your marketing, you need to do similar things to make sure you are GDPR compliant:

1) *Be clear with individuals why you need their data at the point of collection*
2) *Always use clear and concise language appropriate for your target audience*
3) *Give individuals control over their data. They should be able to decide whether to share their personal data with you or not.*
4) *Under the GDPR principle accountability you should be able to demonstrate that you are compliant. This means recording the legal grounds for processing an individual's personal data.*

2 Consent

Asking for consent

- [ ] We checked that consent is the most appropriate lawful basis for processing
- [ ] We asked for consent prominently and separately from our terms and conditions
- [ ] We asked people to positively opt-in
- [ ] We didn't use pre-ticked boxes or any other type of consent by default
- [ ] We used clear, plain easy to understand language
- [ ] We explained why we want the data and what we're going to do with it
- [ ] We gave specific options to consent and to the different types of data processing we carry out
- [ ] We named our organisation and third parties the data may be shared with

  This may be a requirement in the ICO's consent guidance so think about how you would manage it.
- [ ] We told individuals they can withdraw their consent
- [ ] We told the individual they can refuse to consent without detriment
- [ ] We don't make consent a precondition of our service
- [ ] If we offer online services to children, we only ask for consent if we have age-verification and parental consent measures in place.

Recording consent

- [ ] We keep a record of when and how we got consent from the individual
- [ ] We keep a record of exactly what they were told at the time

Managing consent

- [ ] We regularly review consent to make sure that the relationship, the processing and the purposes have not changed since consent was given
- [ ] We have the means to refresh consent at appropriate intervals, including any parental consents
- [ ] Using privacy dashboards or other preference-management tools is good practice
- [ ] We make it easy for individuals to withdraw their consent at any time, and show them how to do so
- [ ] When consent is withdrawn, we act as soon as we can
- [ ] We don't penalise individuals who want to withdraw their consent

Whether you rely on consent or legitimate interests for your marketing, you need to do similar things to make sure you are GDPR compliant:

1) *Be clear with individuals why you are collecting their data*
2) *Use clear and concise language appropriate for your audience*
3) *You must give information at the point you collect data. It cannot be hidden in small print.*
4) *Give individuals control over their personal data. They should be able to decide whether to share their personal data with you or not.*
5) *You should be able to demonstrate your GDPR compliance so record the legal grounds used for processing an individual's personal data. For example, taking a screenshot of the tick box a customer agreed to online and the correct version of the corresponding privacy policy or notice. If an individual challenges you, you will need credible evidence to prove your compliance.*

Credit to the Information Comissioner's Office (ICO) GDPR consent guidance: www.ico.org.uk

3 Information provisions

When collecting personal data you will need to make sure individuals are aware of the following:

- [ ] The identity and contact details of your organisation
- [ ] Contact details of the data protection officer, if you have one
- [ ] The consent or legitimate interests necessary for data processing and why
- [ ] If your organisation uses legitimate interests legal grounds to contact individuals then this must be explained
- [ ] Which third parties data may be passed onto
- [ ] Other countries outside the EU the data may be processed
- [ ] How long the data will be stored, but if that is not possible, then the criteria used to determine that period
- [ ] Tell individuals about their right to have their personal data deleted or rectified, and to object to data processing in the future
- [ ] The right to complain to the national data protection authority, which is the Information Commissioner's Office (ICO) in the UK
- [ ] If a statutory or contractual law requires an individual's personal data
- [ ] Information about automated decision making, including profiling. Organisations should explain, "Meaningful information about the logic involved" in the profiling.

4 Third party data

When buying third party data, make sure you do your due diligence. The GDPR makes you accountable and responsible for making sure the personal data you use for marketing is compliant. To be sure, give third party data suppliers rigorous checks.
You should:

- [ ] Know how the list was compiled

  If an organisation withholds this information then do not use them

- [ ] Know whether the consent was recently obtained/updated
- [ ] Make sure that the third party can prove consent (see point 1)
- [ ] Ask whether data has been screened against the Telephone Preference Service and/or Mailing Preference Service. If not, you will need to screen the data.
- [ ] Make sure your organisation was specifically named when the data was collected

  This may be a requirement in the ICO's consent guidance so think about how you would manage it.

- [ ] See a sample of the data

Record this process so you have proof that you've carried out extensive due diligence of your third party data suppliers.

5 Profiling

Profiling means evaluating personal data so you can make predictions about an individual or group. Marketing communications can then be targeted and personalised for individuals or groups.

- [ ] Tell people how and why we profile personal data but give people the chance to opt-out
- [ ] Explain how you profile an individual's personal data in your privacy notice/policy

If you process personal data via automated decision making then:

- [ ] Consent may need to be explicit - an informed opt-in like a tick box with clear copy explaining any consequences for individuals (see point 1)

If the profiling has legal or other 'significant effect' on individuals

- [ ] You need explicit consent
- [ ] Undertake a privacy impact assessment to determine whether legitimate interest or consent, is the most appropriate legal basis for your profiling activities

6 Legacy data

To continue marketing to individuals on your database, you must make sure that data is GDPR compliant. You will have to satisfy the requirements mentioned in the consent, legitimate interests and information provision sections of this checklist above.

As long as the data you use is GDPR compliant then the ICO will have confirmed that the data can be used after May 2018.

To get your legacy data GDPR compliant:

- [ ] Demonstrate to individuals why you have collected their data
- [ ] Say this in clear and concise language appropriate for your target audience
- [ ] Give individuals the chance to object to the processing of their data
- [ ] Because you should be able to demonstrate compliance with GDPR, you should record your legal grounds for processing an individual's personal data
- [ ] Demonstrate you have clearly and specifically informed the individual what you are doing with their data and why. If cannot demonstrate this, you cannot prove your legacy list is compliant.
- [ ] Reconnect with people on your database using direct mail

  This is your legitimate interests and does not require consent
- [ ] Renew consent at least every two years once you've reconnected