

A closer look at



Transparency

The General Data Protection Regulation

Important

This document is part of a series, produced purely for guidance, and does not constitute legal advice or legal analysis.

All organisations that process data need to be aware that the General Data Protection Regulation may apply directly to them.

The responsibility to become familiar with the GDPR and comply with its provisions from 25th May 2018 onwards lies with the organisation.

Legal advice, if required, should be sought from a Manx advocate.

Index

TRANSPARENCY - THE NEW REQUIREMENTS -----	5
Personal data obtained directly from the individual-----	7
Personal data obtained from a third party-----	8
Transparency requirements - summary -----	10
TRANSPARENCY PRACTICALITIES	
The identity and contact details of the controller -----	12
The contact details of the Data Protection Officer-----	12
The controller’s representative in the EU-----	12
Categories of personal data -----	13
Recipients or categories of recipients -----	13
Purposes for processing personal data -----	13
The legal grounds for processing -----	14
Relying on “legitimate interests” as a ground for processing -----	15
Processing Special Categories of personal data -----	18
The legal grounds for processing Special Categories of personal data -----	19
Processing of personal data relating to criminal convictions and offences -----	20
Retention periods -----	21
Details of international transfers of data outside the EU -----	22
Automated decisions and profiling -----	23
WORKING TOWARDS TRANSPARENCY & CREATING EFFECTIVE PRIVACY NOTICES	
Using privacy notices effectively -----	26
Working towards transparency-----	27
Privacy notices - selecting an approach-----	28
Changes in processing?-----	29
Privacy notices - summary-----	30
Privacy notices - example-----	31
RESOURCES -----	35

Transparency - the new requirements

“Transparency” requires a controller to provide individuals with all the information necessary to understand what will happen to their personal data, how it will be protected, how long it will be kept, where it may be transferred to, and know what rights they have in relation to that data.

Controllers are required to provide that information:

- in a concise, transparent, intelligible and easily accessible form
- in clear, plain language adapted as necessary to meet the target audience needs, especially where children, or other vulnerable groups, are concerned
- in conjunction, if needed or desirable, with standardised icons to give an easily visible, intelligible and clearly legible overview of the intended processing

This means that existing ‘fair processing notices’ (incorporated, for example, in documents, online forms, apps, or websites) which are currently set out in ‘legalese’, tucked away in terms and conditions, or of such a general nature that no meaningful information is provided must be replaced.

Transparency expands upon the existing requirements and, although much of the information is similar, some additional information is required. Complying with the new requirements is, therefore, likely to need resources, the level of which will depend on:

- what information is currently provided to individuals
- whether that information is a true reflection of the processing undertaken (a sound knowledge of data flows will be fundamental to make that assessment)
- how that information is currently communicated to the individual.

A controller must provide enough information to ensure that the individual understands the processing and, where appropriate, is able to make informed choices about the processing of their personal data.

What information must be provided, and when, depends on whether the controller obtains personal data:

- directly from the individual (See page 7), or
- from another source (third party) (See pages 8-9)

Transparency - the new requirements

The extent of the information provided to the individual will depend on the risk **to the rights and freedoms of the individual**. The greater the risk posed, the more detailed and informative the information must be. Similarly, the more complex the processing operations, the more thought needs to be put into making the information clear and informative for the target audience.

The manner in which the information is to be supplied has also changed; it must now be **'provided'** to the individual, rather than being 'made available' to them. An individual is also entitled to ask for the information to be provided to them orally.

Such importance is placed on the provision of transparency information that failure by a controller to comply will attract the higher level of financial penalty.



Resources:

UK ICO's Privacy
Notices Code of
Practice

Personal data obtained directly from the individual

TIMING:

- **WHEN THE DATA ARE COLLECTED**

MANDATORY INFORMATION (new requirements are in bold):-

- the identity and contact details of the controller
- **the contact details of the Data Protection Officer** (where applicable)
- **the controller's representative in the EU** (where applicable, i.e. where the controller is not established in an EU Member State)
- the purposes of processing and the **legal basis** for processing (including the legitimate interest pursued by the controller if applicable)
- **any recipients, or categories of recipients, of that data (if any);**
- **details of any international transfers of the data outside the EU, including:**
 - how it will be protected
 - how details of the measures in place to safeguard that data can be obtained

TO BE PROVIDED WHERE NECESSARY TO ENSURE FAIR AND TRANSPARENT PROCESSING -

taking into account the specific circumstances and context in which the personal data are processed

- **how long the data will be stored** (or the criteria used to set this)
- **all the rights of the individual**, including access, rectification, objection and portability
- **the right to withdraw consent where processing is based on consent**
- **the right to complain to a supervisory authority**
- whether it is mandatory to provide the information due to **statutory or contractual obligation**
- What the **consequences** to the individual are of not providing the information
- **the existence of automated decision making including profiling logic and the impact of it on the individual**

EXCEPTION

- Where the data subject already has the relevant information

Personal data obtained from a third party

TIMING:

- **Within a reasonable period of having obtained the data, but within one month; or**
- **If the data are used to communicate with the individual, at the latest, when the first communication takes place; or**
- **If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.**

INFORMATION TO BE PROVIDED (new requirements in bold):-

- the identity and contact details of the controller
- **the contact details of the Data Protection Officer** (where applicable)
- **the controller's representative in the EU** (where applicable)
- the purposes of processing and the **legal basis** for processing (including the legitimate interest pursued by the controller if applicable)
 - Whether it is mandatory to provide the information (**statutory or contractual obligation**)
 - What the **consequences** to the individual are of not providing the information
- **any recipients, or categories of recipients, of that data;**
- **details of any international transfers of the data outside the EU, including:**
 - how it will be protected
 - how details of the measures in place to safeguard that data can be obtained
- **the existence of automated decision making including profiling logic and the impact of it on the individual**
- **how long the data will be stored** (or the criteria used to set this)
- **all the rights of the individual**, including access, rectification, objection and portability
- **the right to withdraw consent where processing is based on consent**
- **the right to complain to a supervisory authority**

Personal data obtained from a third party

EXCEPTIONS:

- The data subject already has the information (for example, where a processor has already provided the information); or
- The provision of such information:
 - is impossible; or
 - would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) (data minimisation, pseudonymisation, anonymisation); or
- The obligation would be likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests by, for example, making the information publicly available.



Transparency requirements - summary

Information to be supplied	Data obtained directly	Data NOT obtained directly
Identity and contact details of the controller and, if applicable, the controller's representative and data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipients or categories of recipients of the personal data	✓	✓
Details of transfers to third countries and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

Transparency practicalities

Transparency practicalities


The identity and contact details of the controller

	<p>Provide:</p> <p>a physical address, an active telephone number and monitored email address</p> <ul style="list-style-type: none">• Similar to requirements for headed paper and email footers, consider adding these contact details to a website footer
	<p>Do not :</p> <p>Use an online "Contact Us" form, or "PO Box" address, without including any other clear and easily accessible information that identifies the controller and its location</p>

The contact details of the Data Protection Officer (DPO)


This should include information allowing individuals to reach the DPO in an easy way.

The name of the DPO is not mandated, but it may be a good practice to include it. It is for the controller and the DPO to decide whether this is necessary or helpful in the particular circumstances (employees and supervisory authorities will need to know the name of the DPO).

	<p>Provide:</p> <p>a dedicated postal address, a dedicated telephone number, and/or a dedicated e-mail address</p> <ul style="list-style-type: none">• consider using a dedicated DPO contact form
---	--

The controller's representative in the EU

In some circumstances Isle of Man controllers who offer goods and services to residents in EU Member States must designate a representative to act on their behalf in one of the EU Member States where those goods and services are offered.

	<p>Provide:</p> <p>a postal address, a dedicated telephone number, and/or a dedicated e-mail address for the representative</p>
---	---

Transparency practicalities

Categories of personal data

A category of personal data is the type of data. This can, for example, be name, address, customer number or unique identifier, online identity, photographic or CCTV images, biometric data such as fingerprints or facial recognition.

The law also specifies “special categories” of data. (See pages 21-22).

As the processing of special categories of data is prohibited except in specified circumstances, notices should be especially transparent about the processing of special categories of personal data.

Recipients, or categories of recipients

A recipient is a natural or legal person to whom the controller will legitimately disclose personal data to.

Transparency requires recipients to be identified and therefore a controller must identify all persons who will be recipients of the personal data.

Where a disclosure to a public authority is required by law in the course of a specific enquiry, there is no need to include that public authority as a recipient.

Purposes for processing personal data

A data subject must be informed about the purposes (or reasons) for processing their personal data. The purposes must be explicit and legitimate and determined at the time of the collection of the personal data.

Where there is more than one purpose for processing, these must be clearly distinguished from each other.

Purposes can be categorised in a way that is understandable in the context of the business and to individuals and could, for example, include staff management, managing the business’s accounts, the use of CCTV or other surveillance equipment, anti-money laundering monitoring, patient records, direct marketing etc..



Tip

An accurate current notification could be used as a starting point

Transparency practicalities

The legal grounds for processing

For each purpose that you process personal data, you must now identify, and explain to data subjects, which legal ground is being relied on and, in the case of reliance on the legal ground of legitimate interests, provide additional information. (See more about legitimate interests on [Pages 15 -17](#))

Processing of personal data, including that processed in accordance with Article 10 relating to criminal convictions and offences or related security measures, but **excluding special categories** of personal data (defined in Article 9 - see pages 22 - 22), will only be lawful if one, or more, of the legal grounds for processing is met.

The legal grounds are:

- A clear and precise legal obligation or duty (i.e. a legal requirement, for example, AML)
- Contractual obligations (e.g. contract of employment)
- Necessary for vital interests (life and death matters, but only if no other basis is available)
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (i.e. a statutory power - know what it is, where it comes from and whether it specifies any "compatible" processing)
- Necessary for the purposes of legitimate interests
- Consent of the individual* (see more in the separate Closer Look guide)

*Special rules apply where information society services are offered to children below the age of 16 (age limit may be set lower in Member State law)

Processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child and the controller makes reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. (Article 8)

Relying on “legitimate interests”

If no other ground for processing can be met for the identified purpose for processing, controllers may consider reliance on “legitimate interests”.

NOTE: Public authorities cannot rely on this ground in the exercise of their functions.

Article 6(1)(f) sets out the full description of “legitimate interests” as follows:

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

(Recitals 47-50 provide further detail and examples.)

To rely on this ground, controllers must be able to identify precisely what legitimate interest of the controller or third party is to be pursued and why it is necessary to process the individual’s personal data for that interest.

If a controller does decide that it is “necessary” to process personal data for the identified legitimate interest, it must:

1. Identify what interests or fundamental rights and freedoms of the individual, which require the protection of their personal data, may be impacted by the processing (consider protection from identity theft and fraud/human rights/privacy etc.)
2. Consider how/if the impact of that processing can be mitigated
3. Justify why the processing is necessary and overrides the identified interests, rights and freedoms.

If legitimate interests is relied upon, the ‘legitimate interest’ must be identified to the individual.




Any decision to rely on this ground in any particular circumstance should, therefore, be properly documented so that a controller can demonstrate that it has given due considerations to all the requirements. (Such detail may be required by a supervisory authority.)

Relying on “legitimate interests”

The considerations documented should therefore include:

- Whether the processing is one-off or routine
- A clear identification of the legitimate interest(s) being pursued by the controller or by the third party that requires personal data to be processed
- An explanation as to why the processing of personal data is “necessary” for that legitimate interest (e.g. why the legitimate interest can only be achieved by processing personal data)
- Identification of the relevant interests, rights and freedoms of the individual taken into account
- What impact the processing will have on those identified interests, rights and freedoms
- How the impact on the interests, rights and freedoms of the individual is balanced against the legitimate interests of the controller or third party, noting in particular any imbalance in power between the individual and the controller, such as employer/employee
- How the legitimate interests of the controller or third party justifies the overriding of those interests, rights and freedoms
- When a review of the decision to rely on this ground for routine processing is to occur to ensure that the processing continues to be ‘necessary’, to consider whether the legitimate interests remain valid, and whether there has been any change in the balance of legitimate interests over time.

Relying on “legitimate interests”

	<p>Examples of legitimate interests referred to in the law include:</p> <ul style="list-style-type: none"> • Processing <u>strictly necessary</u> for preventing fraud • Intra-group internal transfers (subject to third country measures) • Processing <u>strictly necessary and proportionate</u> for ensuring network and information security • Processing which is <u>compatible</u> with the initial purpose for collection (includes archiving in the public interest, scientific or historical research, or statistical purposes)
	<p>BUT:</p> <p>Careful assessment is required including:</p> <ul style="list-style-type: none"> • the reasonable expectations of the individual at the time, and in the context of, the original collection of data from the individual • in respect of any further <u>compatible</u> processing: <ul style="list-style-type: none"> • Any link between the original processing and the compatible processing • The reasonable expectations of the individuals based on their relationship with the controller as to the further use • The nature of the personal data to be further processed • The consequences of the intended further processing for the individuals • The existence of appropriate safeguards in both the original and intended further processing operations
	<ul style="list-style-type: none"> • Exercise caution in overriding the interests and rights and freedoms of the individual • There should be no imbalance in power between the controller and individual

Transparency practicalities

Processing SPECIAL CATEGORIES of personal data

Article 9 states that the processing of special categories of personal data **is prohibited** unless one of the grounds set out in Article 9(2) is met.

The special categories of personal data are defined in Article 9(1) as:

personal data revealing:

- racial or ethnic origin
- political opinions,
- religious or philosophical beliefs,
- trade union membership

and the processing of

- genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Processing will only be lawful if it meets one of the legal grounds for processing set out in the law.

For each purpose that you process special categories of personal data, you must now **identify, and explain to data subjects**, which legal ground is being relied on.

Transparency practicalities

The legal grounds for processing SPECIAL CATEGORIES of personal data

The legal grounds for processing special categories of personal data are:

- Explicit consent of the data subject

or that the processing is **necessary** for:

- Carrying out obligations under employment, social security or social protection law
- To protect the vital interests of a data subject or other individual where the data subject is physically or legally incapable of giving consent
- For the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- For the purpose of preventative or occupational medicine, for assessing work capacity of the employee, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems on the basis of Union or Member State law or a contract with a health professional
- For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- For archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

or the processing

- Relates to personal data manifestly made public by the data subject
- Relates to processing by a not-for-profit body with a political, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

NOTE: there is no “legitimate interests” ground for processing special categories of personal data.

Transparency practicalities

Processing of personal data relating to criminal convictions and offences

This type of personal data is not included as a special category.

Instead Article 10 states:

“Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out

- **only** under the control of official authority
- **or** when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only under the control of official authority.”

Controllers must identify which ground for processing (Article 6(1)) is being relied on. (See page 14)

Transparency practicalities

Retention periods

The new transparency requirement is that the individual must be given information about the period for which the personal data (i.e. in an identifiable format) will be stored, or if that is not possible, the criteria used to determine that period.

The data protection law does not specify any retention periods itself. Retention periods may vary depending on the purpose for processing; some periods may be statutory, others accepted good practice in a particular industry. Different categories of personal data may also be subject to varying time limits for erasure.

Controllers must be aware of what retention periods apply to the personal data they process and set, and comply with, a suitable retention policy. An analysis of the flow of data* could assist controllers in determining relevant retention periods.

The principle regarding retention of personal data states that personal data shall be *“kept in a form which permits identification of data subjects for no longer than is necessary for the purpose or purposes for which the personal data are processed”*.

This does not necessarily mean that data needs to be deleted; if it is **anonymised*** in such a way that re-identification is not possible, that data is not ‘personal data’ and the law relating to the processing of personal data no longer applies to that data.



*** See Resources**

*Know Your Data:
Mapping the 5W's*

*UK ICO - Anonymisation
Code of Practice*

Transparency practicalities

Details of any international transfers of the data outside the EU

If the **controller or processor** intends to transfer personal data to a third country or international organisation, then this must be stated. An explanation of how the individual can obtain further information regarding the safeguards that are in place to protect that data from the controller or processor must also be provided.

State whether the transfer is:

- On the basis of an **adequacy decision** by the Commission in respect of the country or international organisation,

OR

provide details of the **relevant safeguards**. The relevant safeguards listed under Article 46 include:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules
- standard data protection clauses adopted by the Commission
- standard data protection clauses adopted by a EU supervisory authority and approved by the Commission
- an approved code of conduct (Article 40) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
- an approved certification mechanism (Article 42) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights
- Subject to the authorisation from the competent EU supervisory authority, the appropriate safeguards referred may also be provided for by:
 - (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
 - (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Transparency practicalities

Automated decisions and profiling

Where a controller makes **automated decisions** about, or which affect, the individual, they must inform the individual.

Individuals have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Similarly, where a controller undertakes **profiling** that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her, the individual, should be informed of the existence of, and the consequences of, such profiling.

**Working towards
transparency
&
Creating effective privacy
notices**

Using privacy notices effectively

Following good practice in providing privacy notices helps you to deal with people in a clear and transparent way and empower them. This makes good sense for any organisation and is key to developing trust with customers or citizens.

If you empower individuals to manage what you do with their personal data, giving them more choice and integrating preference management tools, such as a privacy dashboard, with your privacy notice you may be able to obtain more useful information from them.

If individuals are able to exercise real choice over what is done with their personal data, you can be more confident that people have provided informed consent for their information to be used, if this is the legal basis you are relying on.

By taking this approach, you are firstly acting more openly and, in a data protection sense, more fairly, but you are also able to use data more effectively.

As digital interaction with consumers becomes the norm, privacy notices should be seen as flexible and deliverable via a number of mechanisms, often in combination. Following the good practice approach described here means that information can be provided at different times and at appropriate points during an organisation's interaction with their customer.

The value of personal data is increasing and technology is rapidly developing. Personal data can be manipulated and used in increasingly sophisticated ways and sometimes on a large scale. Also, individuals often express general concerns about how their information is used but at the same time they often find it difficult to engage with privacy notices. This leaves them uninformed about how their information is being used and sometimes feeling unfairly treated as a result.

Providing meaningful and effective information in this context is an ongoing challenge for organisations but one that they must meet to comply with data protection law.

To get this right, you need to identify the means of communication and the language and tone that is most appropriate to the audience bearing in mind the way that their personal data is being used.

The UK ICO's "Privacy notices, transparency and control - A code of practice on communicating privacy information to individuals" <https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf>

Working towards transparency

Review and (honestly) appraise existing notices

- How is the information currently given to individuals?
- How easy is it for a reasonable person, without any pre-existing knowledge, to find, access and understand the information provided?
- If your target audience is children, or people in vulnerable groups, are they able to find, access and understand what will happen to their personal data?
- How is the information worded? Does it use clear and plain language?
- What information is actually provided?
 - Is it standard wording?
 - Does the information truly reflect what processing is occurring and why?

Do you know, or can you find out, all the information that must now be provided?

For each purpose for processing:

- Do you know where, or from whom, the personal data originated?
- What is the legal basis for processing?
- How long is the retention period? Where is this set out?
- Do you know whether disclosures can be lawfully made to any particular recipient or type of recipient?
- Is any of the processing undertaken jointly with another controller or by a processor?
- Do you make overseas transfers? What safeguards are in place? Are they recorded somewhere and can you explain to individuals what those safeguards are?

Knowledge of data flows and your lawful basis for processing will be fundamental to providing the required transparency information in privacy notices. If you have undertaken an **analysis of data flows*** you may have most of the information needed.

* See “**Know Your Data: Mapping the 5W’s**” for an example - <https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/know-your-data-map-the-5-ws/>

Privacy notices - selecting an approach

Information can be delivered in numerous ways, including:

- Orally - face to face or when you speak to someone on the telephone (it's a good idea to document that you have done this).
- In writing - printed media; printed adverts; forms, such as financial applications or job application forms.
- Through signage - for example an information poster in a public area.
- Electronically - in text messages; on websites; in emails; in mobile apps.

Identify the means of communication and the language and tone that is most appropriate to your audience bearing in mind the way that their personal data is being used; ideally use the same media to collect personal data and give the privacy notice.

Different approaches can be taken:

Layered notices - allow individuals to decide the depth of the information they require at that time

Just in time notices - such as pop-up boxes on online forms explaining why certain personal data is required

Icons and symbols - can be used as part of a layered approach and act as useful reminders that processing is taking place

Privacy dashboards - allows individuals to control the use of their personal data at any time

Mobile and smaller devices - presents additional challenges, but also include functionality that can be exploited effectively



*Consider reading the UK
ICO's Privacy Notices
Code of Practice
(see Resources)*

Changes in processing?

Privacy notices must be reviewed and updated to reflect any changes in processing.

Where a controller intends to process personal data for a different purpose to that for which they were originally collected (as advised to the data subject) the controller **must provide the data subject** with:

- information on the new purpose; and
- any relevant further information that is “**necessary to ensure fair and transparent processing**”.



This information must be provided to data subjects prior to that further processing, irrespective of from whom, or where, the personal data was originally obtained.

Other changes you will need to convey to individuals to ensure that the processing remains fair include:

- new legal obligations or statutory duties that require personal data to be processed
- changes of the identity of the controller or processor
- New, or changes to, overseas transfers.

The main priority will be to ensure that data subjects are kept fully informed so that the processing of their personal data remains fair and they are able to exercise their rights accordingly.


Privacy notices - summary

	<ul style="list-style-type: none">• Up front and honest• Concise, transparent, intelligible, easily accessible• Clear and plain language, suitable for target audience• Accurately reflect the processing• Living document• Monitor, regularly review and update as necessary• May need more than one to reflect different types of processing• Provided when the information is collected from the individual• Provided to the individual before information not collected directly from them is first used• Know what is says - you may need to explain verbally
	<ul style="list-style-type: none">• One size fits all• Done once and forgotten• Convolutd hyperlink navigation• Included in general terms and conditions• Legal language

Privacy notices - example

Guidance on constructing privacy notices, examples of privacy notices and template privacy notices, are readily available on the internet.

The following pages provide some of our suggestions about constructing a privacy notice, these include breaking the information down into relevant sections under clear, user-friendly, headings.

 This symbol will appear where you could consider providing individuals with the option of exploring more in-depth transparency information, for example, by using a layered notice, the use of directional instructions, such as “*click here for more information*”, the use of suitable icons to indicate further information is available, dashboards, or by providing hyperlinks to other resources. Any resources you redirect to should be monitored to ensure they remain relevant and live.

You could also consider providing a short, simple, privacy notice together with a link to the full privacy notice.

As people are entitled to request that you give them a copy of the privacy notice, you could include contact details for individuals to use to make such a request.

You cannot impose any charge for providing a copy of the privacy notice on request unless the request is manifestly unfounded or excessive, in particular if it is a repeated request. You must be able to demonstrate that you were not obliged to provide the copy.

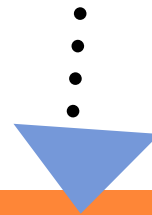
Make it PUCE

Plain language

Uprfront and honest

Clear, concise and appropriate

Easy to find



Tip


Use website footers effectively:

- *to communicate basic information such as controller name and contact details*
- *as a navigation point for accessing privacy notices – you could use an icon, such as illustrated below, instead of the words “privacy notice”*




Privacy notices - example

Who we are

-  The name of the controller and any associated names, such as group companies, group names, website domains or trading names.




Using your personal information

Explain the general reasons for processing personal data, for example what services, facilities etc. are being provided to the individual, or describe any obligations you must comply with that require the processing of personal data (such as AML, credit checks, voter register checks)

-  If you are using personal data for several different purposes, this may need to be broken down and explained clearly.

The information we need ...

Describe/list the types of personal data you need in order to provide the service etc. described above – e.g. name, address, ID requirements.

-  If you are acquiring personal data from third party sources, you should advise the individual.
-  If you are using personal data for several different purposes, this may need to be broken down and explained clearly.
-  If you are relying on **legitimate interests** as the legal basis for processing, you must explain what that legitimate interest is. Further explanation as to how and why the legitimate interests of the controller do not override the interests or fundamental freedoms of the individual may be required.

What we do with it ...


Briefly describe how the information is processed/stored.

The use of processors/cloud services/servers, any third party access, may require further explanation. If transfers are made to third countries, the safeguards for such transfers must be explained.

Privacy notices - example

How long we keep it ...

This information can be extracted from your retention policy - there may be reasons for different retention periods which need to be explained.

 You could provide a hyperlink to your retention policy

Sharing your information



If you do share (or more likely disclose) information, be clear about what you are going to do.

Explain:

- **What** information will be shared
- **Who** it will be shared with
 - Be transparent about 'who' – avoid using general terms such as 'various third parties/ departments' or 'third parties whose products we think you may be interested in'
- **Why** and **when** the sharing may occur
 - the reason for sharing and the consequences of not sharing the information
 - the circumstances when sharing will take place
- **Whether** the sharing requires consent

We would also like to ...

This is where people can be offered the choice to opt in to marketing etc..

For example:

	Yes - I would like to receive offers/updates by EMAIL
	Yes - I would like to receive offers/updates by SMS
	Yes - I would like to receive offers/updates by POST
	Yes - I would like to receive offers/updates by TELEPHONE

Privacy notices - example

Your Rights

Briefly describe the rights of individual (in particular):

- Access to personal data
- Rectification of inaccurate data
- Erasure of data
- Restriction of processing
- Objections to processing

Explain and include the right to opt out from marketing (if relevant):

To exercise any of your rights you can contact us

Suitable-address@your-domain

Your postal address details

AND/OR

To exercise any of your rights you can contact our data protection officer

dpo@your-domain

DPO dedicated telephone number

DPO postal address

If you think we have not complied with your rights, you can make a complaint to the "*relevant data protection supervisory authority name*"



contact details/website for the supervisory authority

Resources

Resources

Significant resources are available on the internet regarding the transparency requirements and privacy notices. Examples of privacy notices and suggested wording and styling are available online, together with webinars.

Whatever method or resource you use, it will be the responsibility of the controller to ensure that the Privacy Notice conveys the required information in a clear and transparent way.

Information Commissioner

Analysis of data flows - "Know Your Data: Mapping the 5W's"

<https://www.inforights.im/information-centre/data-protection/the-general-data-protection-regulation/steps-towards-compliance/know-your-data-map-the-5-ws/>

UK Information Commissioner's Office

"Privacy notices, transparency and control - A code of practice on communicating privacy information to individuals"

<https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf>

"Anonymisation: managing data protection risk code of practice"

<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>

Article 29 Working Party - guidance is expected

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

International Association of Privacy Professionals

<https://iapp.org/news/a/integrating-transparency-into-your-day-to-day-operations-to-be-gdpr-ready/>

GDPR Articles and Recitals

Topic or Area	Article	Recital(s)
Lawfulness of processing - grounds for processing	6	39, 40, 41, 44, 45, 46, 47, 50
Conditions applicable to child's consent in relation to information society services	8	38
Special categories of personal data and grounds for processing	9	51-55
Processing of personal data relating to criminal convictions and offences or related security measures	10	
Transparent information & communication	12	39, 58, 59, 60,
Information to be provided where data are collected from data subject	13	39,58, 60, 61, 62
Information to be provided where data are collected from third party	14	39,58, 60, 61, 62
Transfers subject to appropriate safeguards	46	108, 109, 114

