Guidance on Privacy Statements for Websites

This guidance covers how data controllers can ensure that the collection of personal data through their website is done so fairly and lawfully in compliance with the 1st Data Protection Principle.

This guidance relates to both the Data Protection (Jersey) Law 2005 and the Data Protection (Bailiwick of Guernsey) Law, 2001.

Where the Laws differ and to show differences between the two jurisdictions the page will be split as shown below.

Jersey	Guernsey
Commissioner = Information Commissioner a = article within the Law	Commissioner = Data Protection Commissioner s = section of the Law

Where numbering of passages from the Laws are the same it will be shown as a/s.

July 2016

Table of Contents

What is the difference between a Privacy Statement & a Privacy Policy?

A website Privacy Statement is not a Privacy Policy. A Privacy Policy states how an organisation processes personal data which includes customer data, third party data and employee data. It can, in some instances, be very complex and is fundamentally a document for internal reference.

A Privacy Statement is a public declaration of how an organisation processes personal data on its website. It is a more narrowly focused document and by its public nature should be both concise and clear.

Why do websites need Privacy Statements?

The simple answer is that it is a legal requirement. The 1st Data Protection Principle of the Law states that **personal data must *be processed fairly and lawfully.***

This fair obtaining principle generally requires that a person whose data are processed is aware of at least the following:

- The identity of the person processing the data.
- The purpose or purposes for which the data are processed.
- Any third party to whom the data may be disclosed and other information relevant to the data subject.

Meeting a legal obligation is not the only reason for having a Privacy Statement. Such statements, and adherence to their principles, will promote public confidence and should make such compliant sites more popular with users. Being customer friendly makes good business sense.

What if my website doesn't have a Privacy Statement?

A contravention of the provisions of the Law can result in investigation and enforcement action by the Commissioner. If the Commissioner issues an enforcement notice requiring that you either place a Privacy Statement on your site, or cease processing personal data, failure to comply could result in prosecution with a possible maximum penalty of up to £5,000 (level 4 in

the standard scale) and/or deletion of any/all data collected via the website. Additionally, a/s 13 of the Law gives a person a right to seek compensation from you if that person has been damaged by the manner in which you have processed his/her data.

How do I know if my website requires a Privacy Statement?

If your site does any of the following, a Privacy Statement is required:

- Collects personal data (visitors filling in web forms, feedback forms, etc).
- Uses cookies or web beacons.
- Covertly collects personal data (IP addresses, e-mail addresses).

What information should be contained within a Privacy Statement?

Information should be specific to the processing of personal data on the website. Such information should be sufficiently detailed so as to be useful to the visitor to the site in deciding whether to progress. Statements such as *"all data collected on this site shall be processed in compliance with the Data Protection Law"* are of no value on their own. They need to be accompanied/replaced by an explanation of how, in practical terms, the site complies with its obligations.

Information should include the following:

Identity

Whilst who you are may be obvious to some visitors to your site, you should make sure that you are clearly identifiable. An organisation's name on its own is of little value in this context. Identification should ideally include complete and useful contact details. Useful details would include an e-mail address and postal address that a visitor may use if he/she wishes to communicate with you on any matters relating to the processing of personal data on your website.

Purpose

There can be many overt purposes for which visitors should reasonably expect their data to be used. These may include data necessary in the context of a transaction. However, it is possible that data may be processed for non-obvious purposes such as profiling or future marketing. All these purposes must be clearly referred to in the Privacy Statement. Data volunteered on that understanding are fairly obtained. If a purpose is not obvious and not referred to, then it will be difficult for you to fairly or lawfully process data for that purpose.

Disclosure

If you plan to release personal data to a third party (other than a person acting as your agent) this is a disclosure and must be referred to in your Privacy Statement.

Right of Access

Under a/s 7 of the Law a person has a right to be given a copy of his/her personal data. If you are retaining personal data, you should refer to this Right of Access in your Privacy Statement. You should include reference to procedures to be followed. Under the Law, a Subject Access Request should be in writing, you may charge a fee not exceeding £10 and you must reply within 40 calendar days. Accordingly, you should identify whether you will accept an e-mailed or written request, to whom such a request should be directed and with what it should be accompanied (fee/identification).

Right of rectification or erasure

Under a/s 14 of the Law, a person has a right to have his/her personal data corrected, if inaccurate, or erased, if you do not have a legitimate reason for retaining the data. Your Privacy Statement should make reference to this, if you retain personal data, as well as detailing the procedures a person should follow when making such a request.

Extent of data being processed

If different data are used for different purposes, this should be clearly referred to in the Privacy Statement, rather than a person assuming that all data shall be used for all purposes. This is even more important

in relation to the covert processing of data, such as the collection of IP addresses, use of cookies or web beacons.

Right to refuse cookies

If it is not necessary to use cookies in the context of a transaction, the user should be informed of this and given an opportunity to refuse to have cookies placed on his/her computers. The use of cookies might also be explained to the user.

Is there other information that is recommended to be included?

The previous section details the information that must be included in a Privacy Statement in order to be compliant with the provisions of the Law. However, if you intend that your Privacy Statement is a comprehensive description of your on-line data processing, you may also consider including the following information:

Security

Whilst you are required to have adequate security measures in place to prevent the unauthorised access to, or alteration or destruction of personal data in your possession, any detailed reference to such measures in a publicly available Privacy Statement would be unwise. Rather, you should confine yourself to stating that you take your security responsibilities seriously, employing the most appropriate physical and technical measures, including staff training and awareness and that you review these measures regularly.

Accurate and up-to-date

This is largely a reactive policy, as problems are often only discovered when dealing with the data subject. However, you may make reference to the need to hold only accurate and up-to-date data, suggesting means by which data subjects may update their details or actions you may take to ensure accuracy, such as contacting customers by e-mail.

Adequate, relevant, not excessive

You are required not to hold more data than is necessary for the purpose(s) for which you collect them. Any data in excess of this requirement should either not be requested or, if volunteered, deleted. In a Privacy Statement, you may make reference to a policy to review all data supplied/obtained and delete that which is not necessary, or which is no longer necessary.

Retention

Data should not be held for longer than is necessary for the purpose(s) for which they were obtained. Your Privacy Statement could refer to a policy to delete credit card details once a transaction had been finalised, unless you obtain the consent of customers to retain details to ease further transactions. If you hold different types of data for different time periods, this can also be referred to in the Privacy Statement.

Complaint resolution mechanism

Though not required under data protection legislation, some means of dealing with complaints received from the website's users about data processing would be a customer friendly measure.

Where should I place the Privacy Statement?

A Privacy Statement should be placed in an obvious position and not contained within another document. As a minimum, a Privacy Statement should be easy to spot on the entry page to a website.

Placing a statement only on a Home Page may not be sufficient, as links from other web sites or through search engines may bring a visitor into the site via a page other than the Home Page. The ideal solution to this problem is to place a link to the Privacy Statement on each page. Alternatively, a link could be placed on any page on which data are collected, though if the website uses cookies, this could mean all pages.

Can I place the Privacy Statement within the "terms & conditions"?

A Privacy Statement is a legal requirement and is distinct from terms and conditions, copyright or disclaimer notices. It should stand alone and be clearly identifiable. In order for a Privacy Statement to be of value, it must be readily accessible to the user, quickly read and easily understood. If it is buried within a lengthy document covering a variety of legal issues, it will be difficult for you to demonstrate that you have fulfilled your obligations under the Law.

How often should I review the Privacy Statement?

It should only be necessary to conduct a review if there is some change to on-line processes. However, some mechanism should be in place to notify the appropriate staff member to initiate a review if:

- there is a change to data processing on the website
- there is a planned/actual redevelopment of the website
- there is a new web hosting arrangement
- there are suggestions/comments received from site users.

In any case, the Privacy Statement should be reviewed in the context of an internal audit procedure, which should also review the organisational Privacy Policy, at least on an annual basis.

I am not an IT person, what are cookies?

A cookie is a block of data that a web server places on a user's PC. Typically, it is used to ease navigation through the site. However, it is also a useful means for the website to identify the user, tracking the user's path through the site, and identifying repeat visits to the site by the same user (or same user's machine). This can then lead to a website owner being able to profile an individual user's browsing habits - and all potentially done without the knowledge, or consent, of the user.

How do I know if my web site uses cookies?

This should be a question you address to the person who has developed your website, or to whomever maintains it for you. Most browsers can be set to prevent cookies being downloaded onto a PC. If you set your browser to block cookies, and then visit your own site, you may get an error message displayed if your site is attempting to download a cookie.

Alternatively, you can look into the "cookie" or "Temporary Internet" folder of your PC and see if you can identify a cookie placed by your site. Cookies often, but not always, contain site names.

Do I need to register my company/business with the Commissioner?

Yes, it is a legal requirement if you are processing personal data, unless you are able to take advantage of one of the exemptions for notification.

Do I need to submit my Privacy Statement to the Commissioner for approval?

No, this is not a requirement—but we are happy to make comments on your statement.

What if I use a third party to host my website?

Any person using a third party to host a website should be aware of a number of issues.

Notification

All data controllers processing personal data are obliged to have a current entry in the register maintained by the Commissioner, unless they can take advantage of an exemption to notification. Processing data whilst not having such an entry is an offence. Data processors are under no obligation to notify in respect of their activities conducted on behalf of a data controller. However, it is possible that a data

processor may also be a data controller in their own right and, if so, they are required to notify.

Location of server

If the web hosting service hosts your site on a server outside the European Economic Area, they are obliged to meet at least one of the conditions set out in Schedule 4 of the Law. You, as data controller, should be aware of such trans-border data flows.

Contract

As data controller, you are ultimately responsible to the Commissioner (& the Courts) should the web hosting company unlawfully process data. The 7th data protection principle obliges you to have a contract in writing with the data processor specifying:-

- what the data processor may do with the data on your behalf
- What security measures the data processor must have in place to comply with the 7th Principle.
- That the data processor is only to act on instructions from the data controller.

You must also take reasonable steps to ensure that the data processor complies with these instructions.

Example of a Privacy Statement

It is better to use the term Privacy Statement rather than the term Privacy Policy as the Policy tends to be a very detailed document used internally by an organisation.

Privacy Statements can be short but succinct. The minimum legal requirements to be specified are the organisation's identity, the type of information collected, the purposes for which the information is used, and any third parties to whom the information is disclosed. Individuals must also be informed of their rights to access any data held on them and the right to have it corrected if necessary. If financial details are taken to do a transaction then security assurances may be given in the Statement or at the so called "checkout".

A condensed Privacy Statement may read:

Your personal information is collected from you when you buy a product or request information about our products and services. We keep information on your activity with us, including your visits to our site. (This would apply to the use of cookies)

We use this personal information to deal with your requests, manage your account and offer you other products and services. We respect the privacy and confidentiality of your information and will not disclose it to third parties without your consent unless required to by law.

We use information collected from our website to personalize your repeat visits to our website.

You have the right to see the information that we have about you and you have the right to get any inaccurate information we have about you corrected.

To exercise these choices and rights, write to (insert address), or email (insert e-mail address).

You may opt out of receiving information regarding our products and services from us. You may opt out of receiving offers from others.

Contact the Commissioner

Enquiries and Publication Requests

Jersey

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org