Data Protection Act 2018
February 2019

Information that should be included within the Privacy Notice;

- **The purpose for processing your data**
- **How long we intend to hold the data**
- **If we intend to share your data and with whom**
- **Your rights to your data**
- **Whether we will transfer your data to another country**
- **You right to complain and details of to whom**
- **Business contact details & how to contact**
- **DPO contact details & ow to contact**

Data Matters

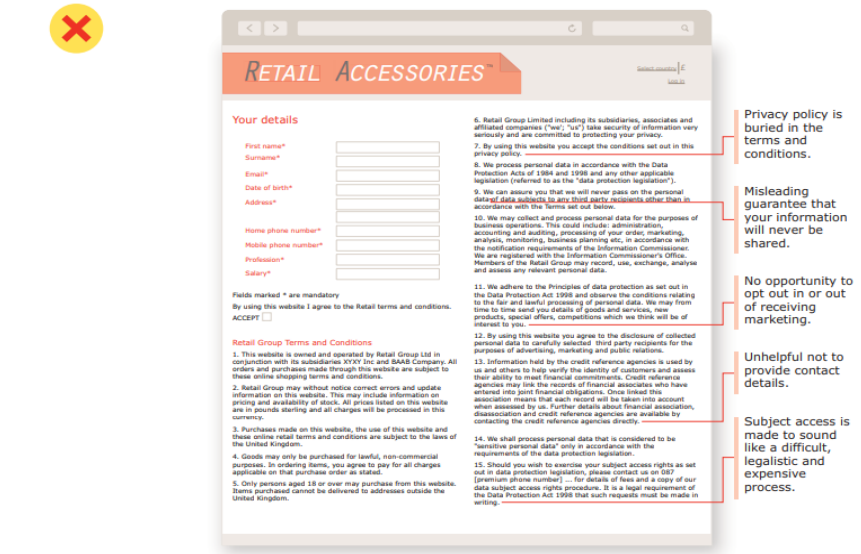
Recap Privacy Notices- Data Protection 2018

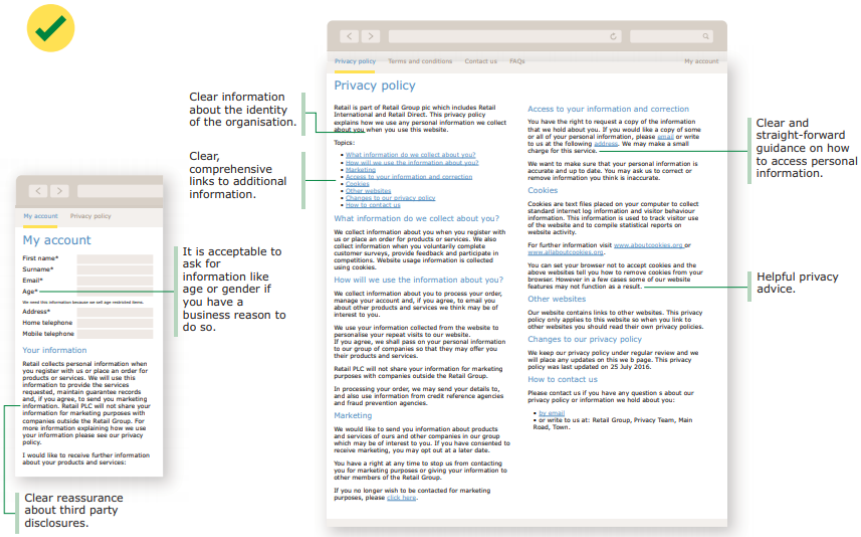
In this issue we will recap on privacy notices and what they mean.

In this edition we will recap on privacy notices. We will look at why these are important, good and bad examples and where to best display these.

Privacy Notices are required to be put in place to notify individuals of how the business will process their data. A privacy notice should be clear and transparent and written in easy to read standard language. Business' should refrain from using legal jargon and keep it simple. If you are a business with a website, these are usually displayed here, however an electronic or paper copy should also be available.

Below are some examples of good and bad privacy notices.





Apex's Data Protection service offers support and advice on privacy notices and other compliance requirements.

Contact Apex for more information on how we can help you stay compliant.

A lot of personal data collected has been freely given by the data subject, for example applying for a job, interest in products and services, subscribing to something, for statutory reasons and many more reasons. This information should be processed for the intended use of which the individual originally supplied it for. The business should not use this information for any other processing type other than originally collected, if the business wishes to process further the individual must be made aware of this and give their consent.

In some very exceptional circumstances further processing will be exempt but this must be assessed against the Data Protection Law exemptions on a case by case basis.

It is also good practice to regularly check and update your privacy notice and by doing so you should keep your stakeholders aware of these changes.

Now is a good time to check if you have a privacy notice in place and make yourself familiar of where to find it. You may want to consider reviewing this and updating your privacy notice.

GDPR and Brexit!

So, the Brexit debate goes on, but where does that leave Data Controllers/Processor in the UK if we leave the EU?

Most business' that operate in the UK may not need to do much to prepare for Data Protection after we leave the EU. The UK is committed to the high standards of data protection set out on the General Data Protection regulations (GPDR). Business' should continue to implement Data Protection standards to comply with Data Protection Laws. The Data Protection Act 2018 will remain in place, the government intends to bring GDPR directly into UK law on exit. There may be some technical adjustments to the UK version, but overall most requirements will remain the same. Upon leaving the EU, any adjustments to the UK Data Protection Law, will mean any policies or documentation may need reviewing and updating and ensuring that key people within the business are aware of any changes.

To find out more information about the ICO, visit their website www.ico.org.uk

The activity carried out by the ICO provides support to ensure Data Controllers/Processors are compliant under Data Protection Laws.

They are there to support but they are also there to enforce if Data Controllers consistently fail to comply with Data Protection Laws and demonstrate Accountability.

The Information of Data Controllers/Processors visited by the ICO and their published reports are freely available on their website.

Activity carried out by the ICO

This month's activity has seen visits to various sectors

These visits have consisted of advisory and audit-based visits from the ICO.

Date of Activity	Identified DC	Type of DC	Type of Visit
4th Jan 2019	Church Lane Primary School & Nursery	Education & Childcare	Advisory
9th Jan 2019	Action 4 Youth	Charitable & Voluntary	Advisory
16th Jan 2019	Dartford and Gravesham NHS Trust	Health	Audit
23rd Jan 2019	`Sussex Police	Criminal & Justice	Follow up Audit
24th Jan 2019	Universities- Overview report	Education & Childcare	Overview report
30th Jan 2019	Greenwood Academies Trust	Education & Childcare	Audit
1st Feb 2019	Active Learning Trust	Education & Childcare	Audit
4th Feb 2019	Surrey Police	Criminal Justice	Audit

The ICO are continuing to carry out advisory and audit visits regularly. The audits that are carried out are to ensure the governance and accountability of data processing.
This reinforces the fact the ICO do visit organisations regularly. So, consistently adhering to the Data Protection Act will ensure your organisation remains compliant.

The audit reports are freely available on the ICO website and they are a useful tool to assess and identify areas for improvement and good practice being actioned followed by other Data Controllers and Data Processors.

Below is an example of some Audit executive summary's, the below is an education and childcare DC and a Criminal Justice DC.

Audit Summary

Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Requests for personal data & data portability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Data Sharing	Limited	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

To find out more information about the ICO, visit their website www.ico.org.uk

These Executive summaries are publicly available on the ICO website. To read more go to the website below;

https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/

Good Practice

It is acknowledged that ALT have focused key resources and taken considerable steps over the last six months to address GDPR compliance. ALT have introduced a number of measures, such as a suite of Information Governance Policies, a GDPR Toolkit, data protection newsletters as well as ICT security audits and IT standards which have made a positive impact on their GDPR compliance. In addition, there is a comprehensive policy and procedure for subject access requests as well as a model letter pack.

Areas for Improvement

ALT should document fully its risk management process, including how risks are escalated.

A programme of regular internal data protection audits should be implemented. Routine compliance checks should be recorded and reported on.

ALT should introduce annual, mandatory information governance training for all staff and report on this as a key performance indicator. Training should include how staff should recognise a subject access request.

Specialist training for key staff in areas such as subject access requests, data sharing, and data protection impact assessments should be introduced.

ALT should document fully its approach to data sharing and record the details of all data sharing and data sharing decisions centrally.

A process for dealing with ad hoc disclosures should be formulated and embedded.

Audit Summary

Audit Scope Area	Assurance Rating	Overall Opinion
Governance & Accountability	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Training & Awareness	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.
Information Risk Management	High	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Areas for Improvement

Although Surrey Police ensures that contracts with processors include the GDPR requirements and that where possible they comply with ISO27001, no compliance checks are carried out to gain assurances that processors have processes to comply with their legal obligations, that processor's provide their staff with data protection training and that staff are aware and understand data protection policies and procedures and that security arrangements are effective and comply with the contract.

Surrey Police currently rely on staff completing the NCALT e-learning to allow them to get an understanding of staff awareness and understanding of data protection regulations. No compliance checks are conducted on a force wide basis to test staff's awareness and understanding of Surrey Police's policies and procedures.

A record of processing activities by Surrey Police's processors is not held.

Surrey Police do not provide any DP training to staff, contractors or volunteers who do not have access to the NCALT e-learning. There may be staff or volunteers on site who may not have access to personal data stored on their computer systems but may be in a position to hear conversations or see sensitive material in regards to personal data.

Although some staff have completed some form of refresher training since they started, some staff were unsure if they had completed any refresher training.

Although Surrey Police have risk assessed their information assets, there is currently no rolling programme for them to be assessed more regularly.

Good Practice

Surrey Police communicate updates of policies and procedures and any new or updated guidance through the use of Routine Orders. It is mandatory for staff to read the Routine Orders as such, all staff members should be aware of any changes to policies and updates to guidance

From the action taken by the ICO on incidents that have happened, it is clear to see the monetary fines that are imposed to those who do not take Data Protection seriously. Since the update, the fines have increased, in comparison to the fines that have been endorsed recently, future penalties will be greater. This can have a detrimental effect on any organisation who do not take their data protection accountability seriously.

Let's not forget the reputational damage this can also have on the organisations. The ICO enforce action against data controllers who do not take data protection seriously and fail to demonstrate compliance.

This Month's 3 Top Tips:

1. When moving away from your laptop or PC, ensure you lock your screen and/or have a timeout screen set.

2. When travelling and using your laptop or mobile phone, be aware of your surroundings, are there people eavesdropping? Or shoulder surfing?

3. Check your passcodes on mobile devices, are they strong enough to prevent unauthorised access?

Enforcement Action

3rd December 2018

A former head teacher has appeared before Ealing Magistrates Court and has admitted two offences of unlawfully obtaining personal data. The head teacher obtained personal information about school children, the information included names, unique pupil numbers, pupil attainment and progress spreadsheets along with performance management data for staff.
The information was obtained from two primary schools at which he had previously worked. The head teacher had stated that he had took the data from the system for professional reasons.
He was fines £700.00, ordered to pay costs of £364.08 and a victim surcharge of £35.00, this was in breach of S55 of the data protection act 1998.

28th November 2018

A former doctor's surgery employee has appeared before King's Lynn Magistrates court and has admitted 4 offences of unlawfully obtaining data. The employee inappropriately accessed the records of patients and staff members. The employee accessed the electronic clinical records of 228 patients and 3 staff members outside of her role as an administration assistant.
The employee was fined £350.00, ordered to pay costs of £643.75 and victim surcharge of £35.00

13th December 2018

A London based firm, Tax returned Limited, was investigated by the ICO between July 2016-October 2017. Their investigation found that they broke the law by sending 14.8 million marketing text messages without valid consent. The firm claimed that some consents were received through generic third-party consent found on privacy policies of certain websites. However, the ICO found that the wording of the policies was not clear and transparent enough, neither Tax Returned Ltd nor the third-party service providers were listed on these privacy policies. The firm has been fined £200,000 by the ICO. Steve Eckersley, ICO's director of investigations said "Firms using third party marketing services need to double check whether they have valid consent from people to send promotional text messages to them. Generic third-party consent is also not enough, and companies will be fined if they break the law".

What is the ICO Registration?

"All organisations, companies and sole traders that process personal data must pay the annual fee to the ICO unless they are exempt"

If you have not registered or have not renewed your registration you could be fined up to a maximum of £4,350.

Find out more about registering on the ICO website,

www.ico.org.uk

Contact Us

32 Macadam Road

Plymouth

PL4 0RU

01752 717610

info@apexhr.co.uk

www.apexhr.co.uk

Finally, in our last edition we asked if you were registered with the ICO? In November the ICO announcement they were beginning enforcement action against those who have failed to register, update registration and pay the fee. Since September 900 notices of intent to fine have been issued by the ICO and more than 100 penalty notices have been issued.

The Fines that are being issued are in the bracket of the following tiers:

1. Tier 1 organisation will be the subject of a £400 penalty
2. Tier 2 organisation will be the subject of a £600 penalty
3. Tier 3 organisation will be the subject of a £4,000 penalty

Organisations across the Finance, Manufacturing and Business sectors are the first to be fined for non-payment of data protection fee.

Finally, Data Controllers

Are you able to confidently demonstrate that you adhere to the 7 principles of the Data Protection Law 2018?

How do you record your compliance?

How confident are you that your staff are aware of the principles and as part of their jobs do, they adhere to these principles?

You no longer have to put off until tomorrow when you can start and act today.

With Apex's help, we have a Data Protection service that can offer you advice and guidance on how to demonstrate your compliance and avoid unnecessary penalties.

So, call or email us at Apex HR and we will support with all of your Data Protection needs.

Check out our Data Protection service on our website.