

# 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.

#### 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
- Your right to complain and details of to whom
- Business contact details & how to contact
- DPO contact details & how to contact



**RETAIL ACCESSORIES**

Your details

First name\*  
Surname\*  
Email\*  
Date of birth\*  
Address\*  
Home phone number\*  
Mobile phone number\*  
Profession\*\*  
Salary\*\*

Fields marked \* are mandatory  
By using this website I agree to the Retail terms and conditions.  
ACCEPT

**Retail Group Terms and Conditions**

- This website is owned and operated by Retail Group Ltd in conjunction with its subsidiaries XXVY Inc and BAAB Company. All orders and purchases made through this website are subject to these online shopping terms and conditions.
- Retail Group may without notice correct errors and update information on this website. This may include information on pricing and availability of stock. All prices listed on this website are in pounds sterling and all charges will be processed in this currency.
- Purchases made on this website, the use of this website and these online retail terms and conditions are subject to the laws of the United Kingdom.
- Goods may only be purchased for lawful, non-commercial purposes. In ordering items, you agree to pay for all charges applicable on that purchase order as stated.
- Only persons aged 18 or over may purchase from this website. Items purchased cannot be delivered to addresses outside the United Kingdom.
- Retail Group Limited including its subsidiaries, associates and affiliated companies ("we") take security of information very seriously and are committed to protecting your privacy.
- By using this website you accept the conditions set out in this privacy policy.
- We process personal data in accordance with the Data Protection Acts of 1984 and 1998 and any other applicable legislation (referred to as the "data protection legislation").
- We can assure you that we will never pass on the personal details of data subjects to any third party requests other than in accordance with the terms set out below.
- We may collect and process personal data for the purposes of business operations. This could include administrative, accounting and auditing, processing of your order, marketing, analysis, monitoring, business planning etc. in accordance with the notification requirements of the Information Commissioner. We are registered with the Information Commissioner's Office. Members of the Retail Group may receive, use, exchange, analyse and assess any relevant personal data.
- We adhere to the Principles of data protection as set out in the Data Protection Act 1998 and observe the conditions relating to the fair and lawful processing of personal data. We may from time to time send you details of goods and services, new products, special offers, competitions which we think will be of interest to you.
- By using this website you agree to the disclosure of collected personal data to carefully selected third party recipients for the purposes of advertising, marketing and public relations.
- Information held by the credit reference agencies is used by us and others to help verify the identity of customers and assess their ability to meet financial commitments. Credit reference agencies may also use the records of financial associates who have entered into joint financial obligations. Once linked this association means that each record of financial associates who have entered into joint financial obligations. Further details about financial associations, disassociation and credit reference agencies are available by contacting the credit reference agencies directly.
- We shall process personal data that is considered to be "sensitive personal data" only in accordance with the requirements of the data protection legislation.
- Should you wish to exercise your subject access rights as set out in data protection legislation, please contact us on 0800 000 0000 or email [privacy@retailgroup.co.uk](mailto:privacy@retailgroup.co.uk) for details of how to make a copy of our data subject access rights procedure. It is a legal requirement of the Data Protection Act 1998 that such requests must be made in writing.

Privacy policy is buried in the terms and conditions.

Misleading guarantee that your information will never be shared.

No opportunity to opt out in or out of receiving marketing.

Unhelpful not to provide contact details.

Subject access is made to sound like a difficult, legalistic and expensive process.



My account Privacy policy

**My account**

First name\*  
Surname\*  
Email\*  
Age\*  
Address\*  
Home telephone  
Mobile telephone

**Your information**

Retail collects personal information when you register with us or place an order for products or services. We will use this information to provide the services requested, maintain guarantee records and, if you agree, to send you marketing information. Retail PLC will not share your information for marketing purposes with companies outside the Retail Group. For more information regarding how we use your information please see our privacy policy.

I would like to receive further information about your products and services.

Clear information about the identity of the organisation.

Clear, comprehensive links to additional information.

It is acceptable to ask for information like age or gender if you have a business reason to do so.

Clear reassurance about third party disclosures.

Privacy policy Terms and conditions Contact us FAQs My account

**Privacy policy**

Retail is part of Retail Group plc which includes Retail International and Retail Direct. This privacy policy explains how we use any personal information we collect about you when you use this website.

Topics:

- What information do we collect about you?
- How will we use the information about you?
- Marketing
- How to contact us

**Access to your information and correction**

You have the right to request a copy of the information we hold about you. If you would like a copy of some or all of your personal information, please email or write to us at the following address. We may make a small charge for this service.

**Cookies**

Cookies are text files placed on your computer to collect information about your browsing habits and to enhance your website usage. This information is used to track visitor use of the website and to compile statistical reports on website activity.

**Other websites**

Our website contains links to other websites. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policies.

**Changes to our privacy policy**

We keep our privacy policy under regular review and we will place any updates on this web page. This privacy policy was last updated on 23 July 2018.

**How to contact us**

Please contact us if you have any question about our privacy policy or information we hold about you:

- By email to: [retail@retailgroup.co.uk](mailto:retail@retailgroup.co.uk)
- By writing to us at: Retail Group, Privacy Team, Main Road, ...

Clear and straight-forward guidance on how to access personal information.

Helpful privacy advice.

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 (GDPR). 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.



## 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
4 <sup>th</sup> Jan 2019	Church Lane Primary School & Nursery	Education & Childcare	Advisory
9 <sup>th</sup> Jan 2019	Action 4 Youth	Charitable & Voluntary	Advisory
16 <sup>th</sup> Jan 2019	Dartford and Gravesham NHS Trust	Health	Audit
23 <sup>rd</sup> Jan 2019	'Sussex Police	Criminal & Justice	Follow up Audit
24 <sup>th</sup> Jan 2019	Universities- Overview report	Education & Childcare	Overview report
30 <sup>th</sup> Jan 2019	Greenwood Academies Trust	Education & Childcare	Audit
1 <sup>st</sup> Feb 2019	Active Learning Trust	Education & Childcare	Audit
4 <sup>th</sup> 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](http://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.

To find out more information about the ICO, visit their website [www.ico.org.uk](http://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.

Active Learning Trust – ICO Data Protection Audit Report – January 2019



### 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.



Surrey Police – ICO Data Protection Audit Report – January 2019

### 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



Surrey Police – ICO Data Protection Audit Report – January 2019

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

### 3<sup>rd</sup> 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 taken the data from the system for professional reasons. He was fined £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.

### 28<sup>th</sup> 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

### 13<sup>th</sup> 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](http://www.ico.org.uk)

## CONTACT US



32 Macadam Road

Plymouth

PL4 0RU

01752 717610

[info@apexhr.co.uk](mailto:info@apexhr.co.uk)

[www.apexhr.co.uk](http://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.

***This publication is for information purposes only and does not constitute legal advice.***