Student ID number: 231 050 854

Supervisors name Garry A. Gabison

Case study Title:

Compliance Handbook: Designing a Website Privacy Policy in Adherence to Privacy Laws

(Tods, Toys and Tea) (3T's)

Word count: 4887

Compliance Handbook:

Designing a Website Privacy Policy in Adherence to Privacy Laws

(Tods, Toys and Tea) (3T's)

Table of Contents

Introduction

This handbook summarises the information necessary for your business to create a compliant privacy policy for your store website. Compliance with the data privacy laws will aid in the

strengthening of your business reputation. It will also help you stay out of legal and financial trouble.

Does this handbook apply to you?

This handbook is directed at the staff of 3T's who deal directly with the website, such as the IT department, and the marketing team who deal directly with customer information. This handbook is also directed at the managerial level staff of the company.

How to use this handbook?

The staff of 3T's (Tods, Toys and Tea) must read this handbook very carefully and comply with it at all times. It must be consulted regularly. In cases of doubt, consult the compliance officer of the firm.

How is this handbook divided?

The handbook is divided into three portions.

- **The first portion** of the handbook explains what is meant by private information in the context of processing. This section also defines key data privacy terms to aid further understanding throughout the handbook.
- **The second section** maps out, under clear headings, a guide to designing a privacy policy that ensures compliance with privacy laws. These headings include controller identification, data collection, user rights, legitimate interests, data security and third-party arrangements.
- **The third section** will go over steps to take in instances of non-compliance, and the consequences thereof.

Section 1. Defining Personal Data and Understanding other Key Terms

- **Personal data-** this is any information that relates to an identified or 'identifiable living individual.

  - An identifiable living individual is a living person who can be directly or indirectly identified by reference to an online identifier such as name.

  - Examples of personal data include:

    + Location data

    + Name and surname

    + Home address

    + ID card number

- What is NOT personal data?

  - Anonymised data- Data rendered anonymous that a person is no longer individually identifiable, so far as the anonymisation is irreversible.
  - Company registration number

- Email with company name as domain

Other key terms to be understood regarding data privacy:

- **GDPR / UK GDPR** (Principal data law):
- **Processing-** Processing (in relation to information, is defined as an operation or set of operations which is performed on information or sets of information, such as;

a. Collection, recording, organisation, structuring or storage
b. Adaptation/ alteration
c. Retrieval, consultation or use
d. Disclosure by transmission, dissemination or otherwise making available.
e. Alignment or combination
f. Restriction, erasure, destruction

- **Data subject –** The quantifiable living individual to whom the personal data relates

- **Data Controller**- A data controller may be a legal person, public authority agency, or an individual (i.e., consultant, self-employed professional, sole trader).

  A controller is responsible for making decisions about data processing activities. They are the person who are obliged to determine the purposes and means of processing data.

- **Data Processor-** The law recognises that agents involved in processing of data have varying degrees of responsibility. A data processor has less responsibility in complying with the data protection laws.

  A processor is defined as a natural or legal person, agency, or other which processes personal data on behalf of the controller. Processors act under the authority of the controller.

  Example: a self-employed barrister is working on a high profile case. He gives the information to a printing business to print. The printing shop is acting here as the processor. The self-employed lawyer is a data controller for the purpose of handling his client's information.

Section 2. Step by Step- Guide to designing a compliant privacy policy

What is a privacy policy?

A privacy policy /notice is a **document** that is the responsibility of the data controller, which sets out **necessary information** in instances of collecting personal data. It is a tool that mainly **communicates** to the **data subject** the ways that your organisation uses personal data, in order to empower them to understand your policies and exercise their rights.

To illustrate this, a children's website adjusts the communication to capture their audience.

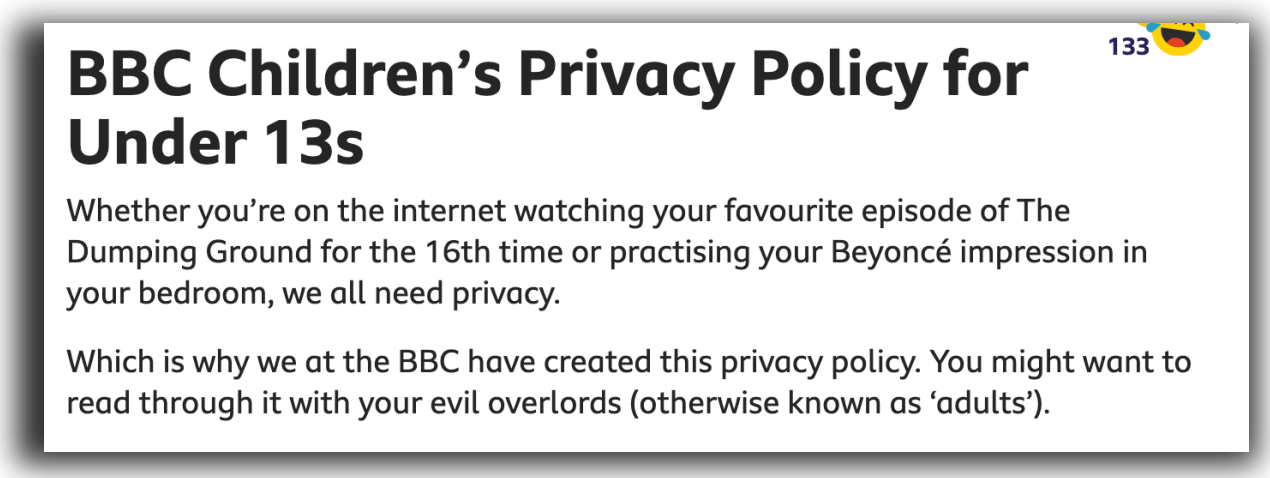


Figure 1: Example of BBC website for children, capturing their audience to communicate privacy

This handbook is a guide to creating a clear policy that will communicate to the data subjects of 3T's, all the necessary information regarding the processing of their private information.

Ensuring privacy compliance means making sure that your privacy policy reflects requirements of current data privacy laws.

- It must be written in **plain and understandable language**.
- It must clearly **identify the data controller** and other processing parties.
- It must **show** the **transparent, lawful and fair** ways you process information
- It must clearly identify **data subjects rights** and means of contacting you, the controller
- It must be **regularly updated** to reflect any changes in law to remain compliant

What should be included in a privacy policy?

Your privacy policy must include the following details. It may follow the headings as listed.

1. ***Controller identification and scope of processing***
2. ***Data collection and use***
3. ***Legal basis for processing data***
4. ***User rights***
5. ***Third party activities***
6. ***Data security***

S 2.1 Controller Identification

Who is the data controller?

To start, you must introduce 'Tods, Toys and Tea' (3T's) as the data controller.

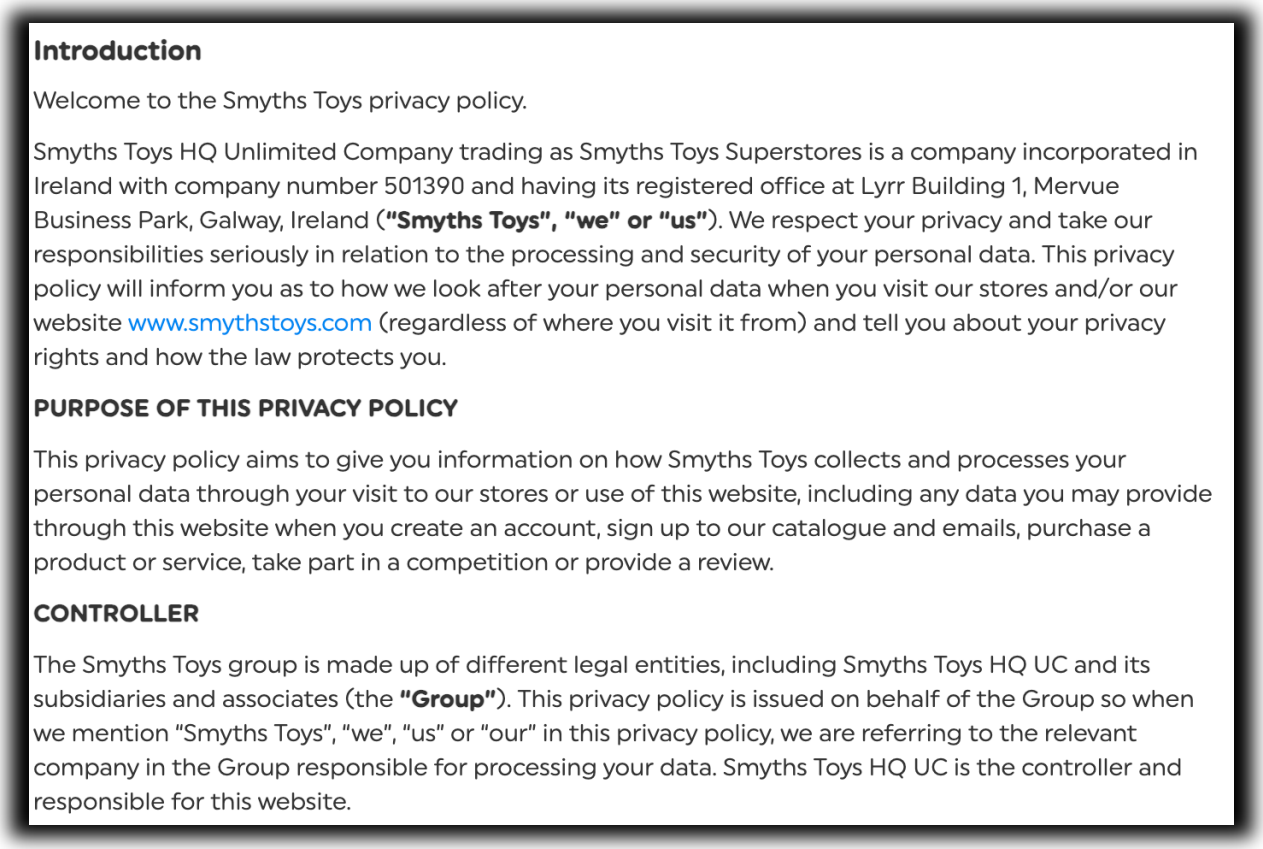
You must include:

- organisations name and clarification of identity
- postal address, email address and any other means by which you may be contactable.

You may include:

- the scope of your processing activities, i.e. when customers visit your stores, website activities etc

The picture in *Figure 1* provides an example of controller identification and scope of processing from 'Smyths Toys' privacy policy.



Introduction

Welcome to the Smyths Toys privacy policy.

Smyths Toys HQ Unlimited Company trading as Smyths Toys Superstores is a company incorporated in Ireland with company number 501390 and having its registered office at Lyrr Building 1, Mervue Business Park, Galway, Ireland (**"Smyths Toys", "we" or "us"**). We respect your privacy and take our responsibilities seriously in relation to the processing and security of your personal data. This privacy policy will inform you as to how we look after your personal data when you visit our stores and/or our website www.smythstoys.com (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

PURPOSE OF THIS PRIVACY POLICY

This privacy policy aims to give you information on how Smyths Toys collects and processes your personal data through your visit to our stores or use of this website, including any data you may provide through this website when you create an account, sign up to our catalogue and emails, purchase a product or service, take part in a competition or provide a review.

CONTROLLER

The Smyths Toys group is made up of different legal entities, including Smyths Toys HQ UC and its subsidiaries and associates (the **"Group"**). This privacy policy is issued on behalf of the Group so when we mention "Smyths Toys", "we", "us" or "our" in this privacy policy, we are referring to the relevant company in the Group responsible for processing your data. Smyths Toys HQ UC is the controller and responsible for this website.

Figure 2: Example of clearly identified controller and scope of processing.

S.2.2. Data collection

How do you collect data?

Next, the law requires that you communicate the kind of information you collect and through what methods they are collected.

- ***What data do you collect and how?***

By law, your policy must communicate the kinds of personal data you use and the particular contexts in which you collect them. They include:

‘Personal information’

Collected by way of user disclosure. Usually collected in the context of profile creation, customer service communications, newsletters, online forum responses etc

- Name
- Address
- Email address
- Username
- Password
- Social media logins

Automatically collected information

Usually collected for service provision purposes. i.e. location specific services, website engagement tracking services etc.

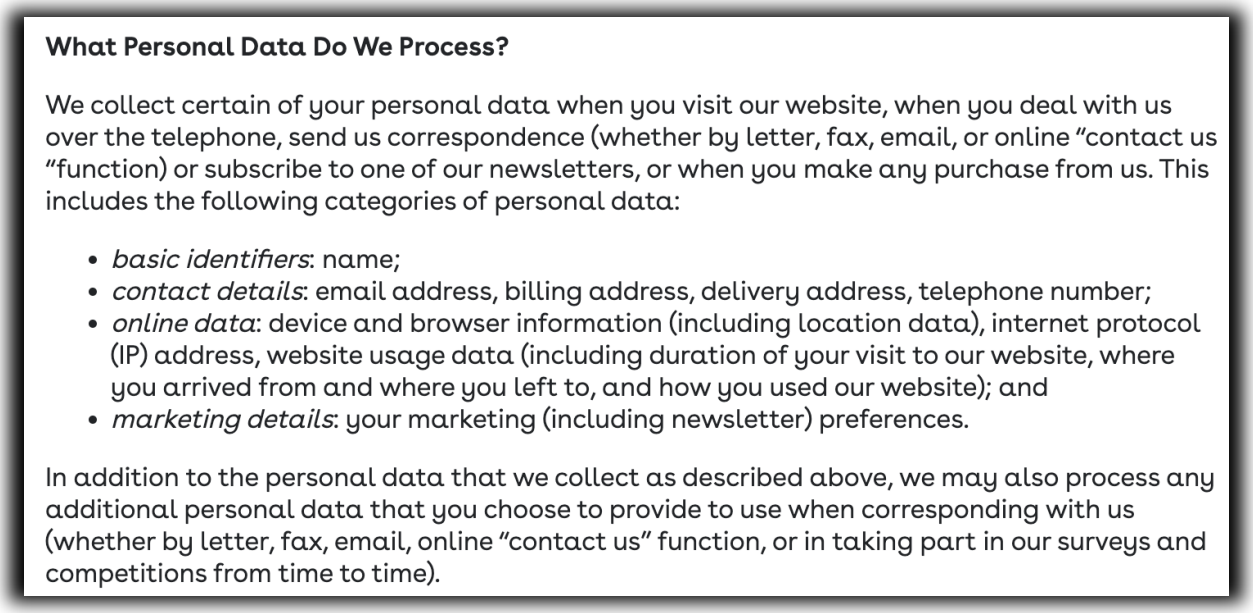
- IP address
- Diagnostic data – Log and usage data
- Location data

‘Sensitive’ information

Must be collected with consent from the users. Usually collected in verification contexts for purchases or age restricted materials.

- Financial data
- Age
- Sex
- Religion

Figure 2 is an example of ‘Toys R Us’ company communicating the kinds of information collected in their privacy policy. This may be used as a formatting example



What Personal Data Do We Process?

We collect certain of your personal data when you visit our website, when you deal with us over the telephone, send us correspondence (whether by letter, fax, email, or online “contact us “function) or subscribe to one of our newsletters, or when you make any purchase from us. This includes the following categories of personal data:

- *basic identifiers*: name;
- *contact details*: email address, billing address, delivery address, telephone number;
- *online data*: device and browser information (including location data), internet protocol (IP) address, website usage data (including duration of your visit to our website, where you arrived from and where you left to, and how you used our website); and
- *marketing details*: your marketing (including newsletter) preferences.

In addition to the personal data that we collect as described above, we may also process any additional personal data that you choose to provide to use when corresponding with us (whether by letter, fax, email, online “contact us” function, or in taking part in our surveys and competitions from time to time).

Figure 3:: Example of ‘Toys R Us’ company communicating the personal data they collect and how they are used.

S.2.3. Lawful basis for processing

How is your processing justified by law?

Next, in order to process personal information lawfully, privacy law requires that your privacy notice explains that you follow one or more legal basis or lawful reasons for processing. The lawful basis given by law include:

- Consent – processing is based on the freely given consent of the user.
- Legitimate interest- based on the justifiable interests of the controller.
- Contract- justified by the fulfilment of a contract
- Legal Obligation- necessary to fulfil a legal obligation. i.e. verification]
- Public Interest- justified by the fulfilment of a public authority function.
- Vital Interest- justified by the protection of the vital interests of users (life or death)

- **As a toy company dealing online for ecommerce and marketing purposes, (3 T's) your lawful basis may follow this guide:**

    a. ***Contract***
        - *Provision of goods and services, including the use of personal information to process orders of products and fulfil them, and process payments.*

    b. ***Consent***
        - *Information given by users consensually may facilitate- marketing communications, newsletters, and other specifically communicated*

purposes. ***Privacy policy must speculate that it may be withdrawn at any time***

c. ***Legitimate interests***

- *Processing may be based on legitimate interests such as – using information to maximise business operations*
- *Derive data to improve web metrics*
- *Advertising and marketing to grow audience and methods such as profiling to deliver targeted experience*
- *Processing information for security and frauds prevention reasons*

You may also adopt a chart approach to presenting your legal basis. The following image is an example of 'Build a Bear' Company's legal basis communication from their privacy notice:

What we collect:	We may use your information for the following purposes, based on the following legal grounds:	Recipients:
• first and last names; • email address; • postal address; • date of birth and/or age; • phone number; • sex/gender; • credit card information; • payment details; • product preference; • purchasing history;	• **If it is necessary for the performance of our contract or for the purposes of entering into a contract:** for the purpose of negotiating and entering into contractual agreements with you, in the course of providing our Services or to enable you to make an in store or online purchase. • **If it is in our legitimate business interests to do so:** for internal record keeping for administration purposes, for the purpose of communications in relation to establishing a customer relationship, including to suggest products and services which may of interest for you, obtaining evidence of identity of our customers, for insight purposes (e.g. to analyze market trends and demographics, and develop the service which we offer to you or other individuals in the future) or for online age verification purposes. • **Compliance with a legal obligation:** in order to prevent fraud or money laundering or to comply with any other legal or regulatory requirements.	1. We may share information about you within the Build-A-Bear group, as more fully described above. (click here for more information). 2. Please note that personal information we are holding about you may be shared with and processed by: 2.1. regulators or other third parties for the purposes of monitoring and/or enforcing our compliance with any legal and regulatory obligations, including statutory or regulatory reporting or the detection or prevention of unlawful acts; 2.2. credit reference and fraud prevention agencies; 2.3. any third party in the context of actual or threatened legal proceedings, provided we can do so lawfully (for example in response to a court order); 2.4. other parties and/or their professional advisers involved in a matter where required as part of the conduct of the Services;

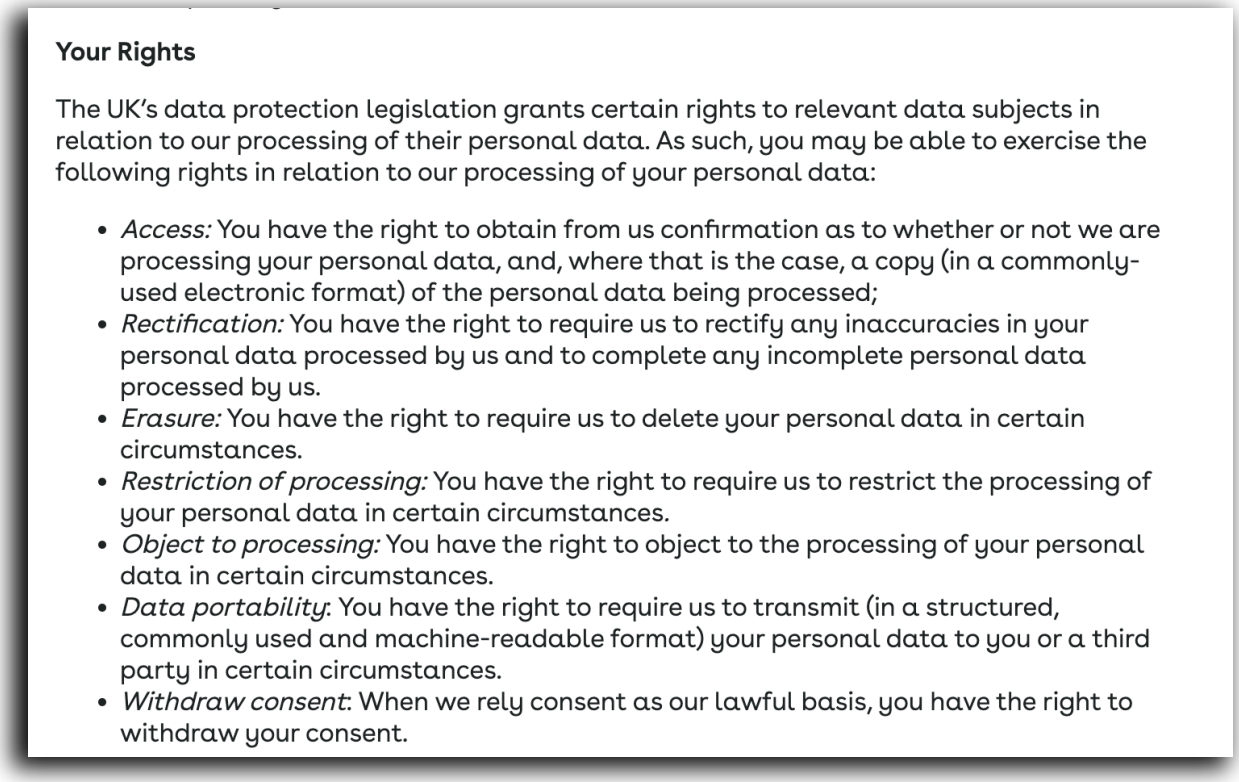
Figure 4: An example of presenting legal basis in online privacy notice by 'Build a Bear' company.

S.2.4 User Rights in regard to personal information

How do you demonstrate user rights?

Next, enshrined by the data laws, your privacy notice must clearly direct users to understand their rights in relation to their personal data. They are given by law as follows:

1. **Right to access-** Individuals must be able to access copies of their personal data.
2. **Right to rectification or erasure-** Individuals must be able to request the rectification of incorrect or incomplete personal information. They also have a right to be 'forgotten' or erased from data systems.
3. **Right to restrict the processing of personal information-** Individuals have a right to restrict or limit the processing of their information.
4. **Data portability rights-** the right to request personal information used, is returned in a machine-readable format, and/or transferred to another company.
5. **To not be subject to automated decision making –** as controller, you must facilitate the right to opt out of automated decisions such as profiling.
6. **Right to objectivity-** Individuals have a right to object the processing of their data for marketing reasons, including the right to withdraw consent.



Your Rights

The UK's data protection legislation grants certain rights to relevant data subjects in relation to our processing of their personal data. As such, you may be able to exercise the following rights in relation to our processing of your personal data:

- *Access:* You have the right to obtain from us confirmation as to whether or not we are processing your personal data, and, where that is the case, a copy (in a commonly-used electronic format) of the personal data being processed;
- *Rectification:* You have the right to require us to rectify any inaccuracies in your personal data processed by us and to complete any incomplete personal data processed by us.
- *Erasure:* You have the right to require us to delete your personal data in certain circumstances.
- *Restriction of processing:* You have the right to require us to restrict the processing of your personal data in certain circumstances.
- *Object to processing:* You have the right to object to the processing of your personal data in certain circumstances.
- *Data portability*: You have the right to require us to transmit (in a structured, commonly used and machine-readable format) your personal data to you or a third party in certain circumstances.
- *Withdraw consent*: When we rely consent as our lawful basis, you have the right to withdraw your consent.

Figure 5: An example of 'Toys R Us' website illustrating the rights of users on their privacy policy.

- ***These rights are facilitated by***

  - ***the inclusion of the controller's contacts details in the privacy policy***
  - ***the inclusion of your resident Data Protection Officers details***

S.2.5. Third party arrangements/ Data Sharing

Does your processing involve other controlling parties?

Next, your privacy policy must outline the measures taken by your firm (3T's) in the arrangement or procedure of data processing in third party arrangements.

- ***International Transfer arrangements***
  - Demonstrate sufficient legal protection
  - Outline purpose of data transfer i.e. additional services
- ***Third party activities and tracking services***
  - Cookies, advertising, social media and commercial sites
  - your policy should outline the kinds of third-party data arrangements you may engage and the purposes of processing under them

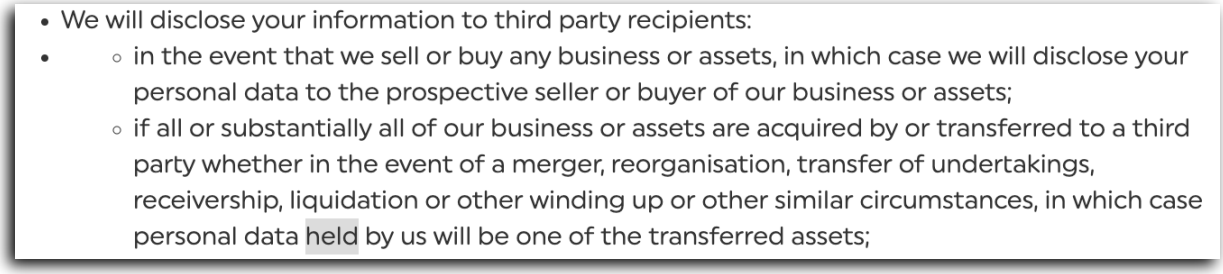

- We will disclose your information to third party recipients:
- in the event that we sell or buy any business or assets, in which case we will disclose your personal data to the prospective seller or buyer of our business or assets;
- if all or substantially all of our business or assets are acquired by or transferred to a third party whether in the event of a merger, reorganisation, transfer of undertakings, receivership, liquidation or other winding up or other similar circumstances, in which case personal data held by us will be one of the transferred assets;

Figure 6: Example from 'Smyths Toys store' illustrating how they frame their communication of third-party agreements.

S.2.6. Data security

Finally, your privacy policy must outline the appropriate measures put in place by your firm to ensure protection of personal information from loss, destruction, misuse or any risks to personal data during processing.

- ***Protective measures***
  - Encryption of data
  - Anonymisation of data

- Data handling policies communicated throughout organisation
- Disclaimers regarding how data is handled by the controller

- ***Limitation of processing***
  - Need to know basis
  - Storage limitation
  - Purpose specific – limited to the particular purpose that data was collected for

This information may be included in the policy under its own heading, followed by disclaimers and notices explaining your procedure. For example, the below image is captured from the 'Build a bear' websites policy.

Personal Information Security

Build-A-Bear Workshop maintains appropriate technical and organizational security measures designed to help protect against unauthorized or unlawful processing, loss, destruction, damage, misuse, and alteration of Personal Information collected by Build-A-Bear Workshop, which include:

- physical and logical access controls, including firewall, limited access, and SSL encryption technology, that limit who can access Personal Information based on business/processing need;
- privacy policies for Personal Information and for employee Personal Information (a copy of which may be requested at privacy@buildabear.com);
- annual employee training on our privacy policies;
- employees who are bound by confidentiality obligations;
- the appointment of a Privacy Officer to handle all Personal Information incidences or issues, including, without limitation, the handling of individual requests related to his/her Personal Information processed by Build-A-Bear Workshop; and
- Build-A-Bear Workshop's General Information Security Policy and Incident Response Policy that contain incident response plans for escalation and resolution of data breach incidents.

All Personal Information collected via our websites is stored on secured servers.

Figure 7: Example of 'Build a Bear' Company's privacy policy, data security section

Section 3. Non-compliance

Understanding your data protection obligations as controller is key to avoiding getting fined, losing your job or sanctioned. Failure to comply with the data laws in creating and managing a privacy policy may mean that you fail to adequately safeguard the personal data you process, or you may not be processing the data lawfully.

You must regularly consult this document to ensure that you maintain a compliant data privacy policy.

Enforcement of the data laws in the UK is carried out by the Information Commission. In cases of non-compliance, you are likely to face;

- Warning notice from the Commission
- High Fines of varying amounts

Figure 8: consequences of non-compliance with the data laws

Designing a Website Privacy Policy in Adherence to Privacy Laws
(Tods, Toys and Tea) (3T's)-**Legal Justification**

This document contains the legal basis and justifications for the instructions given by the handbook, *'Compliance handbook- Designing a privacy policy in compliance with privacy laws.*

The purpose of this handbook is to ensure that as a company operating online for ecommerce and marketing purposes, you are handling the personal data of your customers in a way that is compliant with the data privacy laws. Complying with this handbook means designing a referential framework, the 'privacy policy' which will inform the ways that you collect, store and dispose of personal data. This handbook is based on the governing laws:

- **EU General Data Privacy Regulation (GDPR)**
- **UKGDPR**
- **The Data Protection Act (2018)**

New Stricter approach to handling personal information

The handbook is based on the legal changes leading to stricter handling of personal information in the UK. The main legislative Instruments of data protection in the United Kingdom are the **UK's Data Protection Act 2018** and the **EU's General Data Protection regulation (EU) 2016/679 (GDPR)**[1] adapted to the UK in the form of the **United Kingdom Data protection regulations (UKGDPR)**.[2] These replace the former EU law, the 1998 European Data Protection Directive 96/46 EC and the Data protection Act 1998.

Following the UK's separation from the EU via Brexit, the Introduction of the UKGDPR is an 'adequacy decision', meaning that it casts the UK as adequate for the continued free flow of information with the EU.[3] It may be read in the same way, save for some UK tailored sections like national security.

The GDPR is an update to the former EU law that spotlights data protection in ways such as protecting data subjects from automated decisions, the outlining of their rights,

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation) (Text with EEA relevance)**

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data **(United Kingdom General Data Protection Regulation) (Text with EEA relevance)**

[3] Ibid s 45

and the implementation of thorough consent procedures.[4] It also provides central standards for processing personal data such as its principles. Included here is 'lawfulness', the requirement for an organisation to have a lawful basis for processing personal data.

The replacement the EU Data Protection Directive was initiated by concerns relating to the poor enforceability and compliance with its provisions, and the need for refinement regarding certain concepts.[5] For instance, the directive did not hold a data processor independently liable for their actions. rather, the controller in that situation carried sole liability for processing decisions.[6] The GDPR however ensures that both parties are liable in a processing situation. Additionally, personal data was not well defined in the directive,[7] as it was made limited to actual information types, i.e. names, photos etc. The GDPR on the other hand refines this to include any 'identifiable data', thus enabling the legal coverage of data markers such as IP addresses.[8]

The Data Protection Act 2018 amends the Data Protection Act 1998. It is referred to as a complete 'data handling framework',[9] introduced to help the UK cope with the

[4]Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98,
[5] Ibid
[6] Sahar Bhaimia, 'The General Data Protection Regulation: the Next Generation of EU Data Protection' (2018) 18 LIM 21
[7] Ibid
[8] N-2 recital 30
[9] Department for Digital, Culture, media and Sport, 'Data Protection Act 2018 Factsheet – Overview' (Department for Digital, Culture, media and Sport, 23 May 2028)< https://assets.publishing.service.gov.uk/media/5b07df82e5274a63a50b567e/2018-05-23_Factsheet_1_-_Act_overview.pdf > accessed 30 June 2024

changes in an increasingly digital world. Its key provisions aim to safeguard the rights of the data subject, build protections for the processing of sensitive information, put stringent controls on processing children's information, and empower the Information Commission's enforcement powers to ensure compliance.[10] The legislation is supplementary to the GDPR in the way that it applies its standards and provisions, such as the key definitions used, and the principles of processing personal data.

Section 1. Personal Data and other Key Definitions

The guidance given by the handbook applies to the handling of personal data. This section of the handbook defines personal data and other key terms necessary to understand the handbook such as, processing, data subject and data controller.

These definitions are found in article 4 of the GDPR. Personal data adopts a broader meaning under the GDPR compared to the former directive. The GDPR has evolved to include 'online identifiers' such as IP addresses, cookies and location data.[11]

Section 2. Step by Step- Guide to designing a compliant privacy policy

[10] Ibid
[11] UK GDPR, recitals 26 & 30

The handbook section on designing a legally compliant privacy policy provides what to include in a document that complies with the data laws. It first defines the role of a privacy policy in ensuring compliant data handling practices. It is a document that communicates a company's data handling methods on their website.

The significance of a privacy policy according to the GDPR is that it facilitates the transparency principle of the GDPR. The principles, contained in article 5, must inform every aspect of data processing.[12] Transparency is clarified as the provision of measures which are 'concise, intelligible, clear, easily accessible…clear and plain language'.[13] A privacy policy is a written form of that measure according to article 25's 'technical and organisational measures'[14] The GDPR recital 60 underscores the significance of such measures, highlighting the right of the data subject being sufficiently informed to ensure transparent processing. This includes children.[15]

To this end, the handbook gives an example of the BBC's privacy policy for children, where it adopts child appropriate measures in language, to facilitate their understanding as data subjects.[16]

This handbook section further outlines headings following the themes that must be provided in order to 'design' a complaint privacy policy. These include data collection, data use, legal basis for processing data, rights of the data subject, third party arrangements, and data

[12] UK GDPR s.5
[13] Ibid recital 42
[14] Ibid s.25
[15] Ibid recital 60
[16] British Broadcasting Network (BBC), 'BBC Children's Privacy Policy for Under 13s' (BBC, 2024) <https://www.bbc.co.uk/cbbc/findoutmore/childrens-privacy-policy-u13> accessed 30 June 2014

security. These headings are modelled according to article 14 of the GDPR,[17] which lists the kind of information that must be provided to users where personal data have **NOT** been collected, this is the focus of the handbook, as privacy policy is only a notice. This measure enables the controller to *demonstrate* compliance instances of processing personal information.

i. Identification of Controller

The handbook section on controller identification gives instructions on how the staff of 3T's may identify as controller in a privacy policy. This must be done at the start and include details such that the controller is contactable. I.e. email and postal address.

This is given by the GDPR in article 14 (a), which requires the controller to provide this information for the use of the data subject.[18]

To illustrate this instruction, the handbook uses an example from 'Smyths Toys Superstore' to show how they identify their controller with clarity.[19]

ii. Data Collection

[17] N-6 s.14
[18] UK GDPR s. 14 (a) *Information to be provided where personal Information have not been obtained from the data subject*
[19] Smyths Toys, 'Privacy Policy' (Smyths Toys Superstore, 2024) < https://www.smythstoys.com/uk/en-gb/privacy-policy> accessed 30 June 2024

The handbook section on data collection concerns instructions on the requirement to demonstrate to the user, via their privacy policy, the kinds of personal data collected by the controller and how.

Under article 14 (d) of the GDPR, controllers are obliged to inform the data subject about the data concerned in the processing activities it will undertake.[20] The privacy policy handbook covers both personal information, and sensitive information. Additionally, it outlines that this information may be collected via channels such as verification, marketing communications, etc.

Personal information is the first that must be specified in a privacy policy. It is defined by the GDPR under article 4 as any data that makes an individual 'identifiable".[21] The GDPR builds on the former directive by including online identifiers such as IP addresses and cookie data and location data within the definition of personal data.[22] This allows for increased protections of data identified with natural persons. As such, these bases also cover automatically collected information as outlined by the handbook.

Sensitive Information about persons must also be outlined. This is defined under article 9 as data that may reveal race, ethnic origin, religion and biometric data for example.[23] The GDPR takes a prohibitory approach to this data, which means that controllers must fulfil one of the lawful bases for processing under Article 9 (2) before they can process this information. In a privacy policy a controller must make clear that they require consent to process this data.

[20] UK GDPR s.14 (d)
[21] Ibid s. 4 (11)
[22] Ibid. recital 30
[23] Ibid s.9

The example given under this handbook section is taken from 'Toys R Us' company's privacy policy to act as a demonstration for the web development staff who will implement this workbook.[24]

iii. Lawful basis for processing

The handbook section on lawful basis instructs that the controller must explain their lawful basis for processing personal data within their privacy policies. This means that they must ensure they have legally justifiable reasons to process personal data. This follows the principle of 'lawfulness' of processing under article 5.[25] Lawful bases are defined by article 6. They include consent, legitimate interests, contract, legal obligation, public interest and vital interest. The handbook provides their definitions. In addition,

Within the handbook, it was determined that Tods, Toys and Tots (3T's) would be relying on lawful basis of contract, consent and legitimate interest, as they are a Toy store processing information for marketing and ecommerce purposes. This also follows the guidance to legitimate interests given by the Data and marketing association.[26]

[24] Toys R US, 'Toys R US: Privacy Statement' (Toys R Us, 26 June 2024) < https://toysrus.co.uk/pages/privacy-statement#:~:text=We%20do%20not%20intend%20to,have%20a%20lawful%20basis%2C%20or > accessed 30 June 2024

[25] UK GDPR s.5

[26] Data and marketing association, 'GDPR for Marketers: Consent and Legitimate Interests' (DMA, 2019) < https://dma.org.uk/uploads/misc/new-gdpr-for-marketers_consent-and-legitimate-interest-final.pdf> accessed 30 June 2024

Contract as a lawful basis determines that processing personal information is lawful where it is necessary for the performance of a contract. This is explained in recital 44 of the GDPR.[27] In addition, this basis remains consistent with the former directive.[28] The handbook gives examples of this processing situation, such as the use of personal information to take and process product orders.

Next consent as a lawful basis means that under the conditions of 'freely given, specific and informed' consent from the data subject,[29] their data may be processed lawfully. Furthermore, the GDPR lays a framework of what constitutes valid consent under article 7[30]

- Must be demonstrable
- Consent matters must be clearly distinguishable from other matters contained in the written policy/ notice
- Must be made to be freely and easily withdrawn
- Must be unambiguous- must require a clear opt in rather than a more passive method.

Situations that require consent in the handbook include the facilitation of marketing communications, such as newsletters.

Finally, legitimate Interests according to the GDPR is the lawful basis where processing is legitimised by the controller's interests. The GDPR in recital 47 lists marketing as one of these interests.[31] The handbook lists examples in line with this, such as maximising business

[27] UK GDPR recital 44
[28] A&L Goodbody, 'The GDPR: A Guide for Business' A&L Goodbody 2016; page 14
[29] UK GDPR s.4.11
[30] Ibid. s.7
[31] Ibid recital 47

operations, improving web metrics and advertising such as profiling to deliver targeted services.

In considering legitimate interests, a controller must determine the purpose of processing the data, the extent of the necessity of this act, and whether they balance these interests against those of their data subjects, particularly children.

Finally, this section included an image example from the privacy policy of 'build a bear' to aid implementation.[32]

iv. User rights

The handbook section on user rights gives the instruction that the rights of the data subject must be included in the privacy policy. This section also includes an example to demonstrate how the staff of 3 T's may implement it into their policy.

The rights of the data subject must be included in a privacy policy according to article 12, in order to facilitate the data subjects in exercising them.[33] The rights are 6 in number, provided under article 15 - 21 of the GDPR. they include the right of individuals to access their personal data,[34] right to rectification of false personal information, or erasure from data

[32] Build a Bear, 'Build-A-Bear Workshop Global Privacy Policy - effective 31 May, 2024' (Build a Bear, 31 May 2024) <https://www.buildabear.co.uk/privacy-policy.html > accessed 30 June 2024
[33] UK GDPR s.12
[34] Ibid s.15

systems,[35] the right of individuals to have the processing of their personal data restricted,[36] the right to have their data transferred between controllers (portability),[37]the right against automated decision making,[38]and the right to object data processing (objectivity), i.e. the withdrawal of consent.[39]

The significance of these rights enshrined in the GDPR is to empower users to have more control over their data in an increased way since the former directive.[40] By including them in a privacy policy, the article 14 requirement of information to make necessary available to users is fulfilled. The GDPR requires this from data controllers in order to give organisations a responsibility to assist data users in exercising their rights. As stated by the handbook, this is additionally facilitated by the inclusion of the controller's details in the privacy policy, as well as the contact information of the data protection officer (where applicable).

V. Third parties

Under this section, the handbook instructs that the privacy policy being designed must outline its third-party access/ handling arrangements if applicable. This is required of a privacy policy following article 14 of the GDPR.[41]

[35] Ibid s16, s17
[36] Ibid s.18
[37]Ibid s.20
[38] Ibid s.22
[39] Ibid s.21
[40] A&L Goodbody, 'The GDPR: A Guide for Business' A&L Goodbody 2016; chapter 8
[41] UK GDPR s 14 Information to be provided where personal data have not been obtained from data subject

Data sharing with third parties concerns how other organisations and countries may be involved in processing personal data and maintaining safeguards.[42]The significance of this heading is that there is a risk to the quality of protection of data within the UK when data is processed outside its borders, except for the EU which shares the same data protection system, and is termed 'adequate' for data transfers according to article 45.[43] This 'adequacy' must also be established from these third countries or organisations, before transfers may occur.[44]

The handbook lists two instances of third-party involvement that must be outlined in the privacy policy: International data transfers and tracking services, such as cookies. In addition, it gives an example from 'Smyths toy store' to demonstrate how 3 T's may implement this requirement.[45]

vi. Data security

The handbook instructs that the privacy policy, the topic of guidance, is protected by particular measures that must be outlined under a similar heading in the document. These include technical protective measures, and processing limitations. Additionally, it gives an example from the privacy policy of build a bear's website, for a demonstration regarding how this may be implemented.

[42] ICO, 'A guide to international transfers' (Information Commission, 13 October 2023) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/ accessed 30 June 2024
[43] UK GDPR s 45
[44] ibid
[45] Smyths toy store, 'Privacy policy' (Smyths toys superstore, 2024)) < https://www.smythstoys.com/uk/en-gb/privacy-policy> accessed 30 June 2024

Protective measures such as encryption are justified by the GDPR requirement to implement 'technical and organisational measures' to ensure security according to article 32.[46] Encryption is an example given by the recital 83.[47] Other measures include the appointment of a data protection officer, and the 'assurance' of security measures communicated in the policy .[48] The recital dictates that ensuring data security requires the careful assessment of risks inherent to data processing such as 'breach' as described by article 4(12) to include loss, alteration, accidental and unlawful destruction.[49]

Section 3. Non-compliance

This is the final section of the handbook, providing information on the consequences of noncompliance with the data laws in implementing privacy policy. Enforcement is carried out by the UK's data protection commissioner, the Information commission. This occurs through the issuance of information or warning notices, and administrative fines.

The commission is empowered by the UK GDPR to issue warning or information notices. These are clarified and detailed under article 143 of the Data Protection Act 2018.[50] The commission is additionally empowered by the GDPR to impose fines up to £8,700,000 or 2% of annual turnover, or up to £17,500,00 or 4% of annual turnover.[51] These are subject to specific conditions respectively, contained under article 83 of the UK GDPR. They include

[46] UK GDPR s 32
[47] UK GDPR recital 83
[48] A&L Goodbody, 'The GDPR: A Guide for Business' A&L Goodbody 2016; chapter 11, Data Breach and Security
[49] UK GDPR s 4 (12)
[50] Data Protection Act 2018, s 143
[51] Ibid

instances such as where the controller or processor has infringed the provisions of the legislation; intentional or negligent infringement, action taken by the controller to mitigate them, and the categories of personal data under the infringement, amongst others.[52]

In the enforcement of privacy notices in particular, central to this informational measure is the principle of Transparency, facilitated by the informational requirements under Article 14 (1).[53] The commission recently has dealt with a case on these grounds. The case of *Experian Ltd v Information Commissioner*[54] credit reference agency, one of the largest credit reference firms providing services to 50 million plus people in the UK. In this case the information commissioner opened an investigation into its suspicious handling of personal data. They combine data from a variety of public and private sources without direct relationship to the data subjects except where they are Experian customers.

The Information commission found that Experian was creating this data bank for its own purposes without adequate transparency measures according to article 4 and 14 (1) of the GDPR and was therefore in breach of the GDPR.

This was a case where the Information commission specifically targeted the communication of a company's data processing of its users personal data, alleging a purposeful use of ‘unclear’ language, for example trying to dissuade the users from the fact that their data was being shared with political parties,[55] and instead implementing wording measures to advertise their large scale data mining as financially advantageous to the users, such as the

[52] Article 83 (b,c,d) UK GDPR
[53] UKGDPR s 14 (1)
[54] Experian Ltd v Information Commissioner [2023] UKFTT 132 (GRC)
[55] *Ibid* para 18

use of industry language.[56] The commission found further significance in experience non-compliance, highlighting that a failure to communicate the details of data processing does not allow the subjects to exercise their rights such as rights to erasure.

This case ended in the Information commission attempting to impose strict consent requirements, which Experian appealed on the grounds that it would affect their marketing operations to a large extent. The court later found that the commission did not have enough evidence to claim a breach of the GDPR.

This case highlights the importance of businesses adopting the GDPR's compliance by design. This is supported by Lands, who suggests that controllers must factor compliance into modelling their commercial operations.[57] Where a controller is able to build systems which clearly communicate their processing and purposes, maintaining transparent and well communicated data processing operations will come at less cost.

[56] *Ibid*
[57] Robert Lands, 'Experian v ICO: First-tier Tribunal takes fundamentally different view of credit reference agency's marketing services' (2023) 34(4) Entertainment Law Review 134-135

Bibliography

- **Legislation and Case Law**
  - Data protection Act 1998.
  - Data Protection Act (2018)
  - European Data Protection Directive 96/46 EC 1998
  - *Experian Ltd v Information Commissioner* [2023] UKFTT 132 (GRC)
  - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) (Text with EEA relevance)
  - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**United Kingdom General Data Protection Regulation)** (Text with EEA relevance)

- **Secondary sources**
  - A&L Goodbody, 'The GDPR: A Guide for Business' A&L Goodbody 2016;
  - British Broadcasting Network (BBC), 'BBC Children's Privacy Policy for Under 13s' (BBC, 2024) < https://www.bbc.co.uk/cbbc/findoutmore/childrens-privacy-policy-u13 > accessed 30 June 2014

- Build a Bear, 'Build-A-Bear Workshop Global Privacy Policy - effective 31 May, 2024' (Build a Bear, 31 May 2024) < https://www.buildabear.co.uk/privacy-policy.html > accessed 30 June 2024
- Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019) The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, 28:1, 65-98,
- Data and marketing association, 'GDPR for Marketers: Consent and Legitimate Interests' (DMA, 2019) < https://dma.org.uk/uploads/misc/new-gdpr-for-marketers_consent-and-legitimate-interest-final.pdf > accessed 30 June 2024
- Department for Digital, Culture, media and Sport, 'Data Protection Act 2018 Factsheet – Overview' (Department for Digital, Culture, media and Sport, 23 May 2028)< https://assets.publishing.service.gov.uk/media/5b07df82e5274a63a50b567e/2018-05-23_Factsheet_1_-_Act_overview.pdf > accessed 30 June 2024
- ICO, 'A guide to international transfers' (Information Commission, 13 October 2023)< https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-transfers-a-guide/> accessed 30 June 2024
- Robert Lands, 'Experian v ICO: First-tier Tribunal takes fundamentally different view of credit reference agency's marketing services' (2023) 34(4) Entertainment Law Review 134-135
- Sahar Bhaimia, 'The General Data Protection Regulation: The Next Generation of EU Data Protection' (2018) 18 Legal Information Management 21

- Smyths toy store, ‘Privacy policy’ (Smyths toys superstore, 2024)) < https://www.smythstoys.com/uk/en-gb/privacy-policy > accessed 30 June 2024
- Toys R US, ‘Toys R US: Privacy Statement’ (Toys R Us, 26 June 2024)< https://toysrus.co.uk/pages/privacy-statement#:~:text=We%20do%20not%20intend%20to,have%20a%20lawful%20basis%2C%20o > accessed 30 June 2024