Awful NOT LAWFUL

Fulfilment of the GDPR transparency obligation
2018-2020

BiR Business Information Risk Management Consulting

in association with barnesmeridian

Executive summary

Transparency about personal data processing is an essential component of both public confidence and actual compliance with the GDPR‡. It is explicitly referred to in three separate Recitals and is the specific subject of Articles 12, 13 and 14, so it is reasonable to assume that it ranked high on the agenda of legislators when the Regulation was created.

However, as data protection consultants we have been increasingly concerned by widespread apparent failure of businesses both in the UK and elsewhere to fulfil the transparency obligation. To investigate this we collected a large randomly selected sample of privacy notices from public web sites and analysed them in terms of their effectiveness in supporting exercise of data subject rights.

When we embarked on the study we expected to find wide variation both in the adequacy of privacy notices and in the nature of compliance failures. However this turned out not to be the case. We found a small cluster of remarkably consistent specific compliance failures. These seemed to arise from erroneous interpretations of the regulation's requirements, and they made it hard, or at worst impossible, for data subjects to exercise their statutory rights. We found only a very few privacy notices that would assist data subjects reasonably effectively to exercise their rights, and around half the data set included meaningless or unlawful content.

Four very serious (but almost universal) fundamental misconceptions underpinned the overwhelming majority of the identified non-compliance:

- that a privacy "policy" is a contract between the data controller and data subjects, whereas it is actually a statutorily binding unilateral undertaking by a data controller *to* its data subjects;
- that it is sufficient to list examples of personal data processing, whereas it is in reality obligatory to identify every purpose and processing activity individually;
- that it is legitimate to assign more than one lawful basis to a single purpose and processing activity, whereas the lawful basis for each is necessarily unique and is a matter of fact;
- that data protection management is a technology issue, whereas it is over 90 per cent business process management and corporate governance.

Our key conclusion is that, even where businesses have apparently made some effort to fulfil the obligation, implementations of transparency have not been validated as effective. The frequency with which the same fundamental errors occur suggests that there is little real understanding of the legislation, that corporate oversight of compliance is inadequate, and that a lot of bad advice is in circulation. We hope this report, by drawing attention to these common but critical failings, will assist in improving the current poor state of compliance.

BiR Business Information Risk Management Consulting
Mike Barwise BSc, CEng, CITP, MBCS, MCIIS, LCCP, FRSA
Director

Revised July 2021 taking account of C(2021) 4800 final of the European Commission dated 28.6.2021

‡ As the UK GDPR and Data Protection Act (DPA) 2018 reliy on the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council) in respect of obligations to data subjects including the transparency obligation, for simplicity we assume throughout that the requirements of the two are essentially the same, and we generally imply both when using the acronym GDPR or the term Regulation. All specific references to the legislation make use of the EU GDPR Article or Recital numbers.

The study

Purpose and approach

Our aim was to gauge the level of compliance with the transparency obligation under the GDPR, specifically from the perspective of data subjects in the UK. The primary point of reference for members of the public is commonly some form of online privacy statement or 'policy', so we took these as the source of our data.

For a year from July 2018 we collected a sample of such documents from randomly selected web sites offering a wide range of consumer, commercial, professional, social, medical and political services.

The fundamental question we sought to answer in each case was

could a data subject make use of this document to exercise their statutory rights?

To this end we both examined the documents ourselves from a professional standpoint and also sought opinions from members of the public.

We identified an unexpectedly small but consistent set of significant errors of both commission and omission that rendered almost all those examined non-compliant with the GDPR, in that they made it hard, or in many cases impossible, for data subjects to exercise their statutory rights under the legislation.

From July 2020 to mid-January 2021 we revisited the sampled sites to establish whether there had been any improvement

Key Terminology

The privacy related documents we collected were referred to variously by their authors as *privacy policies*, *privacy statements* or *data protection policies*. For simplicity, in this report we refer to all such documents as **privacy notices**. Direct quotes from the Regulation and from privacy notices are presented in italics and enclosed in 'single quotes'.

Our criterion of compliance

Article 5(1)(a) of the GDPR (the first Principle) states (emphasis added):

> *'Personal data shall be:*
>
> *(a) processed lawfully, fairly and **in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency'); '*

and Recital 39 explains what transparency means (emphasis added):

> *'Any processing of personal data should be lawful and fair. **It should be transparent to natural persons** that personal data concerning them are collected, used, consulted or otherwise processed and **to what extent the personal data are or will be processed**. The principle of transparency requires that **any information and communication relating to the processing of those personal data be easily accessible and easy to understand**, and that clear and plain language be used.*
>
> *[...]*
>
> ***Natural persons should be made aware of** risks, rules, safeguards and rights in relation to the processing of personal data and **how to exercise their rights** in relation to such processing. In particular, **the specific purposes for which personal data are processed should be explicit and legitimate** and determined at the time of the collection of the personal data.'*

Articles 13 and 14 set out exactly what information must be provided, but only general guidance on its presentation is offered by those Articles and Recitals that make reference to transparency. Nevertheless, the way the required information is presented can strongly influence data subjects' ability to exercise their rights.

Consequently, while numerous and varied opinions, both legal and lay, have been published on how the required information should be presented in theory, we attempted to discover how well the purpose of the Regulation in relation to transparency is typically fulfilled in practical terms.

It is clear from Article 1(2) that the GDPR is human rights law, not data law. Indeed in addition to Article 1(2), 29 recitals and 32 Articles directly refer to the *'rights and freedoms'* of the data subject and others. These references clearly indicate that the common assumption of the Chapter III rights being the sum total of data subject rights is fallacious. This is borne out by Articles 79 and 82, which allow for judicial remedies and compensation for *material or non-material damage*.

Therefore the conclusion we came to without hesitation was that the purpose of a privacy notice is firstly to allow data subjects to decide whether any *specific* processing of their personal data by the data controller infringes their rights and freedoms, and secondarily to support data subjects in obtaining redress for any such infringement.

Our criterion for compliance of a privacy notice was therefore whether it assists, restricts or prevents the data subject in accomplishing these objectives.

The attributes we considered

We considered the following attributes as representative of the state of compliance, bearing in mind however that partial compliance is not lawful in the case of the GDPR. All the requirements of the Regulation must be fulfilled, so failure of a privacy notice in any respect entirely nullifies it, resulting in non-compliance with the Regulation as a whole.

Accessibility: whether a privacy notice can be found easily on a web page, whether it can be read regardless of the technologies used (including the user's browser settings), and whether it can be printed conveniently for offline reading.

Readability: the length and clarity of the text, the ease with which it can be assimilated in its entirety, and any presence of distracting or irrelevant material.

Validity: whether the relevant content of a privacy notice complies with the specific requirements of Articles 13 and 14, particularly whether all the mandatory information is present.

Specificity: whether the relevant content is organised in a manner that allows data subjects to identify specific processing and the rights they can exercise in respect of it.

Presence of strictly unlawful content: e.g. exclusions of data controller liability or obligation; improper constraints or conditions imposed on data subjects; failures to recognise the legislation.

Limitations of the study

Our sample is necessarily small compared with the vast number of corporate sites on the web. It was selected at random via keyword searches for verticals, although we could not possibly represent the entire range of verticals presenting on the web. Nevertheless, the small range and consistency of compliance failures found gives us reasonable confidence in the general applicability of our findings.

All percentages quoted in relation to the sample size or breakdown are approximate.

Examples

Quotations of web page and privacy notice content have been selected only as representative examples for the purposes of discussion. Nothing else is implied by their selection, and we have taken steps to anonymise them as far as practicable.

Findings

The data set

The data set was accumulated by browsing to randomly selected web sites in specific business and social verticals identified via keyword searches. We acquired a sample of over 400 notionally unique privacy notices making reference to the GDPR (the *data set*) and also noted, but did not include in the data set, around 50 sites where no reference to a privacy notice could be found by expending reasonable effort.

Approximately ten per cent of the privacy notices in the data set referred exclusively to the web site on which they were present, not mentioning any data processing in support of the wider activities of the site owner. Of these, around half referred exclusively to 'cookies'.

On examination, we found many privacy notices that were largely duplicates despite being in use by completely unconnected organisations. This suggested that standard templates (in some cases including much actual content) were being used by multiple businesses in different verticals (and therefore potentially undertaking different personal data processing).

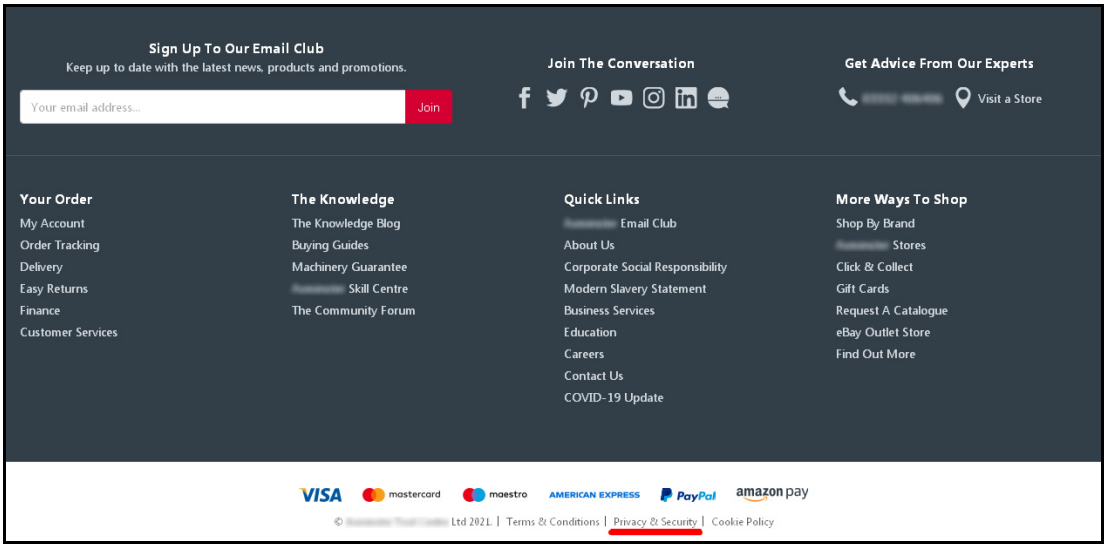
Thirty nine verticals were represented in the final data set (see Annex A). No vertical stood out as better or worse than any other in terms of the compliance of privacy notices; not even, surprisingly, legal services or data protection consultancies.

We classified the origin of the represented businesses on the basis of the declarations found in their privacy notices. Approximately 76 per cent of the data set were from UK businesses, 14 per cent from self-declared multinationals with UK and EU presence, four per cent from EU-based businesses serving the UK, and five per cent from USA based businesses with no obviously declared presence in the EU or the UK. We could not determine the relevant jurisdiction with any confidence from the privacy notices of around one per cent of the data set.

No identifiable country of origin distinguished itself for compliance. Indeed there was negligible difference in the incidence or nature of compliance failures present in privacy notices of UK or European origin and in the "GDPR" sections of privacy notices of multinationals or from the USA.

We ultimately considered that around two per cent of the privacy notices we examined met our criterion of transparency sufficiently to be usable by data subjects in exercising some of their Chapter III rights, although none were entirely transparent throughout.

Accessibility

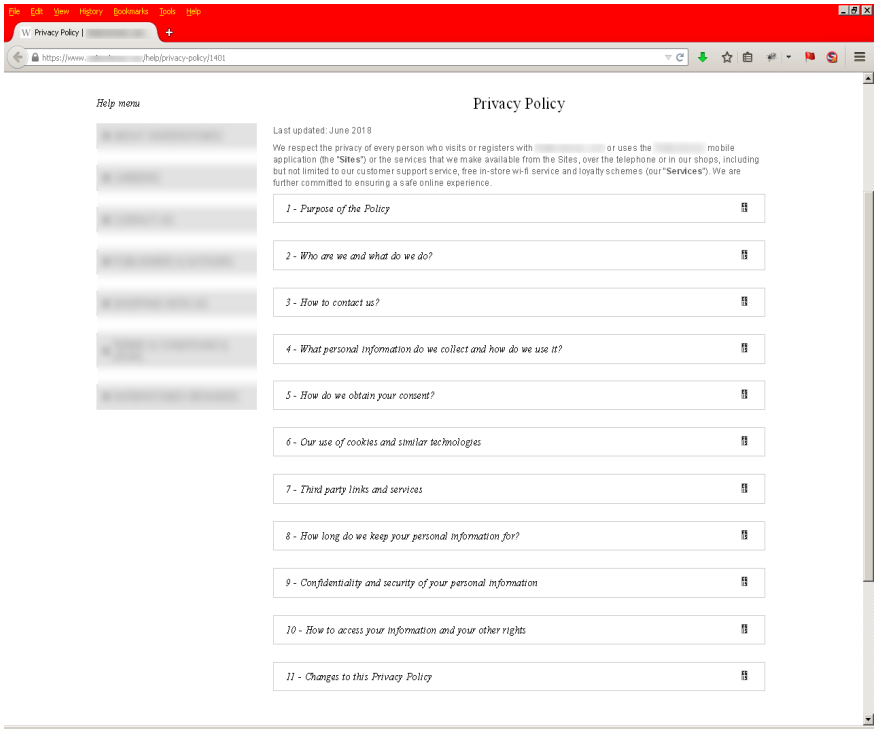


A minimalist privacy policy link (identified by added red underline)

Almost all the privacy notices were quite hard to find, absent prior expectation. The overwhelming majority were linked to at the extreme bottom of an often long web page, usually in a minimally small font (e.g. seven by five pixels for a capital letter). Many were accessed via a "Terms and Conditions" link or were buried within a "Terms and Conditions" document itself. There is clearly a common misapprehension that a privacy notice is contractual, despite the regulation providing for no mutuality. In reality the statutory disclosures under Articles 13 and 14 effectively constitute a unilateral undertaking by a data controller to its data subjects, not an agreement between the parties.

A common barrier to accessibility, particularly relevant to longer privacy notices, was difficulty in printing a hard copy. In some cases banners overlaid the head or foot of every printed page, thereby obscuring part of the text. Quite commonly printing was restricted to the current screen view alone or to only the first printed page of a multi-page privacy notice instead of the entire document. These problems typically appeared to result from use of unsuitable content management system (CMS) templates.

Printing was also rendered impractical in some cases by use of drop down sections within the privacy notice, resulting in only part of it being visible (and thus potentially printable) at any one time.



An unprintable 'drop down' privacy notice

We found multiple examples of JavaScript driven privacy notice links that were thus inoperative unless scripting was enabled. Several of these were on pages containing third party JavaScript trackers that activated as soon as the page was visited, thereby silently breaching the user's privacy before the privacy notice was even readable.

A small number of privacy notice web pages would not even render readably on screen unless JavaScript was enabled. This might make a privacy notice inaccessible to users of technologies such as some text to speech screen readers.

Some privacy notices simply did not exist. Links ostensibly leading to a privacy notice were either dead or led to a blank page. In these cases it commonly appeared that the web site was driven by a CMS. We assume that the template used included a "privacy notice" link by default, but provision of the relevant content had been overlooked.

Readability

We determined the length of privacy notices by copying and pasting the significant content into a text editor equipped with a word count.

Length range (words)	Proportion
less than 1,000	9%
1,000-2,000	16%
2,000-3,000	18%
3,000-4,000	19%
4,000-5,000	14%
more than 5,000	23%

Breakdown of privacy notice lengths

The majority of privacy notices in the data set were more than 2,000 words long, equivalent to at least four average A4 pages of text, and almost a quarter were over 5,000 words long. A small number were of zero length, as links ostensibly leading to a privacy notice were dead (returning "404 Not Found") or pointed to a blank page. Two extreme examples were over 30,000 words long.

Particularly if it could not be printed, even the typical length (four to ten A4 pages) would make a privacy notice hard to fully assimilate prior to using a web site.

We found two distinct approaches to use of language. The most common was plain English replete with vague assurances but lacking in specifics about the processing undertaken, for example

> *'We recognise our duty of care with regards* [sic] *to your data and will always endeavour to do the right thing with the personal data you choose to share with us, including: not compromising your anonymity; protecting your privacy; storing your data securely and giving you control over your own data '*

We suspect that merely *"endeavouring to do the right thing"* would not pass muster as a defence.

At the other end of the spectrum, privacy notices consisted of potentially obscure cross referenced clauses in formal legal language, e.g.

> *'In addition to the other uses and disclosures of information set forth in this Privacy Policy, and notwithstanding anything in this Privacy Policy to the contrary, we may use and disclosure* [sic]*, for any purpose, any Non-Personal Data, except where we are required to do otherwise under applicable law. If we combine any Non-Personal Data with Personal Data, then we will only use and disclose such combined information for the purposes described in sections 4 and 9 of this Privacy Policy while it is so combined '*

Here, *'... anything in this Privacy Policy to the contrary'* confuses by suggesting the reader should search for the *'contrary'*, and uncertainty is further introduced by the reference by "non-personal data". Why mention it at all? The legislation specifically doesn't apply if it is genuinely not personal data as defined by Article 4(1).

Albeit for different reasons, neither of these examples is likely to leave a data subject much the wiser.

Some privacy notices were presented on cluttered pages that included a large amount of extraneous matter. This could include columns of links to other pages, irrelevant images or advertisements interspersed among the text. All of these could distract from the significant content. The cause seems in general to have been the use of a single common CMS template for an entire web site regardless of how it affected clarity of communication on specific pages.

One "privacy notice" consisted exclusively of a block of the meaningless "Lorem ipsum" pseudo-Latin body copy used by graphic designers for page layout.

Validity

Around ten per cent of the privacy notices in the data set referred only to processing that supported use of the web site on which they were posted, in some cases despite the organisations clearly offering services involving personal data processing beyond that limited remit. Particularly in such cases, lists of web cookies tended to dominate the content — by name and even by origin but without significant information about the business purposes they served. This strongly suggests a prevalent but erroneous view that data protection is purely or primarily a technology issue.

No privacy notice mentioning cookies clearly pointed out that they come primarily under European Directive 2002/58/EC — implemented in the UK as the Privacy and Electronic Communications (EC Directive) Regulations 2003 aka PECR. Nor indeed did any fully comply with that Regulation. In only a small number of cases was the distinction made between strictly necessary cookies and other cookies, the use of which would depend on data subject consent. None at all described any mechanism for managing that consent beyond a suggestion that users adjust their browser settings, which would typically not fulfil the purpose. Other types of trackers than cookies (particularly third party script driven trackers) were rarely mentioned, and in no case were they clearly documented. Referral to a tracking third party's privacy notice was the most common approach to "informing" data subjects.

More than half the data set contained superfluous statements with no legal force such as *"We take your privacy seriously"*, often in the absence or partial omission of the actual information required by Articles 13 and 14 of the GDPR. For example, one specimen started with the statement

> *'Our promise: We will comply with applicable privacy and data protection laws and regulatory frameworks.'*

but failed to include the obligatory information in the succeeding text.

One organisation had merely posted online a spreadsheet containing the raw results of what appears to be an internal data protection audit. Supposing it was accurate and complete, the information could strictly speaking be considered valid, but due to the way it was presented it would be effectively useless to data subjects in exercising their rights.

Particularly in respect of data subject rights a significant number of privacy notices did little more than suggest data subjects do their own homework, for example just listing the rights by name, but referring to the Information Commissioner's web site for details.

Commonly, even privacy notices from organisations that appeared to be making some conscious effort to fulfil the requirements of Articles 13 and 14 of the GDPR nevertheless did so in a naïve and non-compliant manner.

These privacy notices consistently addressed each clause of the Articles individually in sequence, rather than considering the purpose of the Articles as a whole. Thus, a list of all the data categories processed would be followed by a list of all the purposes, followed by a list of all the lawful bases relied on. This naïve clause by clause presentation was by far our most common finding in those privacy notices that listed specific data types, purposes and lawful bases at all.

Open ended qualifiers such as *"examples of"*, *"without limitation"* or *"including but not limited to"* in lists of processed data types or purposes were also widely present in these and other privacy notices, clearly implying undeclared, and therefore unlawful, processing.

Both these failings prevent data subjects identifying *specific* processing (each individual cluster of data categories, purpose, processing activity and lawful basis). Unless every specific processing activity is individually and clearly identified with all its associated parameters, data subjects can establish neither whether there is anything objectionable about any of the processing nor which Chapter III rights they are entitled to exercise in respect of specific processing they might object to. This restricts their *statutory freedom* to challenge such processing.

Specificity

Even in the remarkably few privacy notices where the requirement to associate specific purposes, data categories, processing activities and lawful bases appeared to have been at least minimally recognised, vagueness was practically universal. Conflation of multiple loosely expressed but nevertheless clearly (at least to us) incompatible purposes was extremely common.

Type of data	Description	Examples of how we use it
Contact	• Who you are • Where you live • How to contact you	• Servicing your product • Marketing • Analysis & profiling • Enhancing our product and service offering
Personal Details	• Age • Gender • Family details • Visual images & personal appearance • Financial Details • Lifestyle and social circumstances	• Marketing • Analysis & profiling • Policy underwriting

An example of conflated purposes

Depending on how they are interpreted, profiling and marketing could require prior data subject consent, whereas *'servicing your product'* at first sight implies reliance on contractual necessity. The inclusion of *'gender'* and *'lifestyle and social circumstances'* suggests the possibility of processing Article 9 sensitive data for which prior consent is also expressly required for the stated uses. Consequently these categories and purposes should not have been combined, but addressed separately in sufficient detail for a data subject to make informed decisions.

Vagueness as to lawful bases for processing was also almost universally encountered. At worst this consisted of merely listing all possible alternatives provided for by the legislation.

Third party recipient	Purpose of disclosure	Legal Basis for Processing
Independent licensees / franchisees and network providers in order to perform our contract with you and to understand how you use our services and to improve our business	• Make and confirm your rental reservation; • Provide our rewards program and update partner points and rewards; • Connect with your corporate and commercial accounts;	• Performance of Contract; • Legitimate Interests; • Legal obligation; or • Consent.

An example of conflated purposes and lawful bases

Here, all four lawful bases available to the organisation are listed against all the stated purposes. The only ones omitted are *'processing is necessary in order to protect the vital interests of the data subject or of another natural person'* (Article 6(d)) and *'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'* (Article 6(e)), neither of which is likely to be relevant to the data controller's business.

As each of the listed lawful bases attracts different Chapter III rights, data subjects can not establish from this list which rights they can invoke against each of the stated processing activities (in this case, each individual purpose of disclosure). Including all possible lawful bases in association with any single purpose suggests that at the very least the significance of distinct lawful bases has not been understood or has been ignored. In this case confusion is exacerbated by the wording of the *'Third party recipient'* column, which makes independent indirect reference to a lawful basis (contractual necessity).

Another very common error was heading a *"Lawful basis"* column with a legend such as *"Lawful basis including legitimate interest"*, thereby implying that legitimate interest has special status, or that it somehow overrides the other lawful bases. In fact, none of the lawful bases has any special status or priority in law, each applying as a matter of fact to the specific purpose and processing.

In a few cases complete confusion was created by combining open ended lists, conflation of purposes, vague data classifications, assignment of multiple lawful bases, and misleading labelling of entries all at once.

To manage our relationship with you which will include: (a) Notifying you about changes to our terms (b) Asking you to leave a review or take a survey (c) To respond to refund requests and complaints	(a) Identity (b) Contact (c) Profile (d) Preference	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated, to study how customers use our products/services and to respond to you)

The ultimate in confusion

In this example, the three activities in the left hand column are not compatible in terms of the obligations imposed by the Regulation. Descriptors such as *'profile'* and *'preference'* in the middle column are not well defined data categories and therefore convey no useful information to the data subject about what is being processed. Three alternative lawful bases are listed in the third column, and the labelling causes further confusion. It does not correlate across the columns, although superficially it gives an impression of doing so. For example, asking for a customer review (b) might legitimately tie to contact information (b), identity (a) or even preference (d), but it is hard to conceive how it can apply to compliance with a legal obligation (b).

It is clearly still not well understood that as different Chapter III rights attach to the various lawful bases (for example we can object to processing on the basis of legitimate interest but not to that on the basis of legal obligation) only a single lawful basis may be relied on for each specific processing activity. This was pointed out as far back as November 2017 by the Article 29 Working Party (now the European Data Protection Board) in their *Guidelines on Consent under Regulation 2016/679*. The Working Party quite reasonably argued that it should not be permissible for processing on one lawful basis to be continued on another lawful basis if it had been prevented by exercise of a Chapter III right under the first lawful basis. For example, if processing on the basis of consent were terminated by withdrawal of consent, it should not be possible to continue it by invoking legitimate interest instead.

Finally, one privacy notice in our data set included the statement

> *'the Owner will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract '*

That is nice to know, as it is actually a statutory obligation to do so. However, basic diligence would expect a data controller to document this publicly, rather than wait to be asked for it by individual data subjects. This is an important consideration, because a privacy notice is essentially a statutorily binding undertaking by a data controller to its data subjects that the processing undertaken is entirely as specified and exclusively as specified. Indeed amending some aspects of processing, particularly the lawful basis relied on, in a compliant manner can be extremely complicated to achieve, as it is necessary to not only justify the change but also inform all affected data subjects of it, and of how it affects their rights.

Presence of strictly unlawful content

We frequently encountered imposition of obligations on the data subject as a component of, or an enforced adjunct to, a privacy notice. This took various forms, the most basic being an extremely common requirement for visitors to "consent" or "agree" to a privacy notice. In quite a few cases sites were implemented to prevent or obstruct their use unless such agreement were granted by clicking on an acceptance button. As in such cases we never found the privacy notice to be readable in full prior to a user clicking on the "acceptance" button, such demands effectively assumed acceptance by default of unseen terms. Quite apart from being contractually questionable, this contravenes the legal definition of consent.

Requiring consent is unlawful, as consent by definition (Article 4(11)) is (emphasis added)

> *'**freely given, specific, informed** and unambiguous **indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her '*

If processing of personal information is genuinely *required*, three alternative reasons immediately come to mind. It might be necessary to fulfil some legal obligation, whereupon consent is irrelevant. It might be unavoidably necessary for the performance of a service to the data subject, whereupon contractual necessity would be the appropriate lawful basis. Alternatively the information might serve an internal purpose deemed essential by the data controller organisation (e.g. fraud prevention), in which case legitimate interest would be the appropriate lawful basis for its processing. For general commercial enterprises, there are not that many cases where it is necessary or even appropriate to rely on consent.

Another common error is the assumption that data subjects can legitimately be expected to agree in advance to future changes to processing, for example

> *'By submitting this information you consent to use of the information in accordance with this Privacy Policy as amended from time to time.'*

As consent must be *informed* it is impossible to consent to something that has not yet been specified.

Many privacy notices in the data set included imposition of a notional obligation to read the privacy notice, for example

> *'By using [REDACTED]'s services (the "Services") or registering, downloading information or entering the Site and/or the App you acknowledge that you are or have had the opportunity to become aware of this Privacy Policy and [REDACTED]'s practices described therein, including the processing (including collecting, using, disclosing, retaining or disposing) of your information under the terms of this policy.'*

No such obligation exists under the GDPR, which requires a data controller to provide the relevant information, but is silent on whether a data subject should make use of it. Any apparent duty to read the document would be a purely contractual matter between the parties concerned, and so should not be part of a GDPR privacy notice.

A subsequent clause in the same privacy notice attempted to impose an imaginary duty on data subjects to impart its content to third parties

> *'In the event where you provide [REDACTED] with any information regarding another person, you procure that you have made them aware of this privacy policy.'*

There is no such duty under the GDPR. Indeed the Regulation imposes no obligations at all on individuals acting in a private capacity. Therefore this would again be a contractual matter between the data controller and users of its service, which should be made abundantly clear by including it explicitly under *"contractual terms and conditions"* rather than burying it within a privacy notice.

More extreme in the same direction were occasional explicit attempts in privacy notices to transfer liability from the data controller to the data subject.

For example

> *'We may change this Privacy Policy from time to time (for example, if the law changes). Any changes will be immediately posted on Our Site and you will be deemed to have accepted the terms of the Privacy Policy on your first use of Our Site following the alterations.'*

Once again *'you will be deemed to have accepted the terms of the Privacy Policy'* — the erroneous assumption of a contractual obligation imposed on the data subject, but in this case (also erroneously) not on the data controller, as the notice continued

> *'For the avoidance of doubt all policies relating to GDPR and/or data protection (whether referred to on the [REDACTED], the [REDACTED] website or otherwise communicated to [REDACTED]'s staff, members or non-members) are not contractually binding on [REDACTED] and may be withdrawn or amended at any time.'*

The statement *'all policies relating to GDPR and/or data protection [...] are not contractually binding on [REDACTED]'*, while (possibly) literally true by virtue of the word *"contractually"*, is in principle the exact inverse of the reality. Under the Regulation, such "policies", once declared, are *statutorily* binding on the data controller.

A fundamental problem in all these cases is that making acceptance of the content of a privacy notice a contractual obligation might arguably weaken a data subject's right to redress. In principle, if you have consented to the terms of a contract, it is harder subsequently to object to them. Fortunately the *Article 29 Working Party Guidelines on Consent* render the practice non-compliant as it would constitute superimposition of consent on top of any other declared (or indeed actual even if not declared) lawful bases for processing, and enforced consent is in any case disallowed under the GDPR itself. Unfortunately these considerations have apparently failed to register with a very high proportion of data controllers.

The most overt example of such inversions of reality we encountered was, however, a privacy notice with the title and headline

'DATA PROTECTION

exclusion of liability (disclaimer)'

We are unaware of any general provision for *'exclusion of liability'* within the GDPR.

One highly disturbing vertical-specific finding was a small number of almost identical privacy notices on the web sites of UK medical practices and health centres. These universally asserted (emphasis added)

> *'All information held about patients is completely confidential. The Practice is registered under the **Data Protection Act 1984**. This Act protects data held on the computer system.'*

referring of course to legislation that was repealed and superseded a couple of decades ago. On contacting one of these medical centres we were told they used *"a third party to create and manage the web site."* Regardless of who manages its web site, failure by the data controller to identify and correct a fundamental error of this enormity suggests a lack of corporate governance that is serious cause for concern, particularly considering that the majority of the data processed is very probably subject to Article 9.

We traced the origin of these privacy notices to a UK based service provider specialising in web support for medical practices. On alerting them to the error they responded that they would advise *"their IT department"*. Quite apart from the obviously templated stereotyped content of these privacy notices which might well not reflect all the actual processing undertaken in each case, we can only be appalled at the thought of anyone's IT department defining statutory declarations of data processing for third party organisations processing the most sensitive categories personal data.

Some questionable loose ends

In addition to the gross failures discussed so far, across the entire data set we found other examples of non-compliance that arouse concern, for example:

- the privacy notice of a UK based online store stated that in event of exercise of the right to erasure (Article 17) it could not comply but could only mark the record as dead on its database, because, supposedly, deleting records would destroy the database. We have in the past encountered some legacy customer relationship management (CRM) systems on which records could not be irrevocably deleted, but this renders their continued use for personal data processing intrinsically non-compliant;
- despite Privacy Shield having been explicitly struck down in judgement ECLI:EU:C:2020:559 of the European Court of Justice (16 July 2020), several USA based online service providers with world wide coverage apparently continue to rely on it, for example

  'we will continue to abide by Privacy Shield principles'

  This ignores the fact that the Court judged the entirety of privacy Shield invalid specifically because those principles were intrinsically powerless to protect data subject rights in the face of overriding federal legislation.

  However as late as mid-January 2021 the US federal Privacy Shield web site included the statement

  'The U.S. Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List.'

- We note that, while not being bound by ECLI:EU:C:2020:559 as it is not a member of the EU, the Swiss Federal Data Protection and Information Commissioner followed the ECJ on September 8, 2020, issuing an opinion that Privacy Shield is *'insufficient'*. So both jurisdictions in whose interest Privacy Shield was established have formally nullified it. We have nevertheless seen no evidence either from the most recent review of sites represented in the data set that alternative protections such as standard contractual clauses are replacing Privacy Shield, or indeed of any reduction in the use by UK businesses of services that continue to rely on it.

Untrustworthy sources of public guidance

We discovered several sets of privacy notices that were virtually identical despite being presented by very different organisations — indeed in some cases in radically different verticals. This drove us to search for common sources of guidance.

There is a vast accumulation of advice on the GDPR online, but the bulk of it seems to come from questionable sources. We found numerous templates, mostly from sources with no obvious professional standing. Too many for comfort were largely pre-worded documents. A few expected little more customisation than adding an organisation name and contact details.

Unfortunately, even official and quasi-official sources of guidance did not necessarily pass muster. Templates provided by an EU funded GDPR specialist guidance organisation and also by the UK ICO are structured clause by clause rather than by specific processing activity. As previously discussed, this denies data subjects freedom to exercise their rights in respect of specific processing activities.

At least as troubling are online automated "privacy policy generators". One example purported to generate a "privacy policy" for any jurisdiction on the planet, merely from answers to some standard questions in an online form. Its output appeared (from examples traced back to this service via branding) to be essentially a terse statement of clauses from the privacy legislation of the chosen jurisdiction.

Another automated service fronted its offering with a page containing a button labelled *"Generate Privacy Policy in 2 minutes"*. This page included the statement

> *"A Privacy Policy agreement is the agreement where you specify if you collect personal data from your users, what kind of personal data you collect and what you do with that data. This agreement is required by law if you collect personal data."*

We admittedly did not test this (chargeable) service, but we doubt that the personal data processing of almost any organisation could be expressed completely, accurately and compliantly in just two minutes. We also challenge the term *"agreement"* in this description, as a privacy notice is specifically not an agreement between a data controller and data subjects, but a unilateral statutorily binding undertaking by a data controller *to* its data subjects..

While the output of such services might possibly constitute a compliant privacy notice in some hypothetical Utopia, it certainly would not in the EU or the UK. However, many organisations apparently consider the use of such services as absolving them from paying further attention to compliance with Articles 13 and 14.

Unfortunately, the official guidance in the UK still leaves something to be desired. It specifies extensively what the law literally requires but in general provides very limited guidance on how to achieve it — particularly on what might distinguish compliant from non-compliant implementation. Understandably, there can be a perceived conflict of interest for a regulator between enforcement and provision of what might be construed as consultancy, but we believe the ICO currently steers a somewhat too cautious path, leaving the way open for the uninformed to seek and act on guidance from untrustworthy sources. Nevertheless, the 23 per cent of privacy notices in our data set from organisations outside the UK did not fare any better against our criteria for compliance. Consequently, with the notable exception of the ICO template mentioned above, the limitations of UK official guidance are probably not the most significant contributory factor to what actually seems to be an effectively universal failure so far to understand the true purpose of the legislation in respect of transparency.

Two years on

Most of the privacy notices revisited from the last quarter of 2020 onward appeared not to have been updated to any extent. Although wording had apparently been revised in some cases, almost all of these showed only minor changes, and none of the fundamental flaws we identified had been rectified.

Some USA organisations represented in the data set appeared to have recognised that Privacy Shield has been invalidated. Nevertheless even they still seemed in general to rely on it in their privacy notices, we presume unquestioningly following the lead of the US Department of Commerce.

One marked change we observed during the final review in January 2021 was simplification of presentation — specifically, fewer privacy notice pages included extraneous material such as banners, adverts or links to other resources. Plain backgrounds and large fonts now seem to predominate. This can only be a good move in aid of clarity, although this clarity has not yet extended to include the primary links to privacy notices, which remain generally as inconspicuous as before.

Conclusions

Reviewing governance

We are prepared to be generous in assuming that wilful intent to mislead data subjects is rare. In some cases we did however observe apparent intent to evade the responsibilities imposed by the legislation (for example *'DATA PROTECTION exclusion of liability (disclaimer)'*).

Across the entire data set, the overriding source of the non-compliances we identified seems to be failure to understand the real purpose of the Regulation, coupled with insufficient determination to find out.

This confirms our consulting experience in the run up to the GDPR coming into force. Preparing organisations for achieving compliance, we found the majority had not studied, or in some cases even obtained a copy of, the Regulation itself, but had solely sought guidance and training from secondary sources.

From this study, we conclusively established in some cases, and were able to infer in many more, that outsource management was defective. Layout and presentation (and apparently in some cases even content) of privacy notices seems commonly to have been left to the discretion of third party web designers. Where this was apparent, no verification of the adequacy of the deliverables was detectable.

In our consulting we commonly find the IT department responsible for managing data protection compliance. Indeed, the UK government guidance on data protection preparation for Brexit was officially classified under "*digital*". There appears to be a general misapprehension that the GDPR is data law, whereas it is actually human rights law in relation to data processing. This error has inevitably led both to a narrow interpretation of obligations and to assignment of compliance responsibilities to the wrong people.

Although a superficial reading of Article 2(1)

> *'This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'*

might tend to reinforce an assumption that compliance is an IT matter, the corporate IT department is not where GDPR compliance management should come to rest. In reality a lot less than ten per cent of the Regulation's obligations relate to technologies even indirectly, the other 90 per cent or more essentially being matters of corporate governance and business process management.

While the legal department is likely to be the best place to go for interpretation of the Regulation's Articles, it is probably not the ideal source of a privacy notice. Firstly, the fundamental function of a corporate legal department is to protect the organisation, whereas the purpose of the Regulation is to protect the data subject. Secondly, the language in which legal documents are commonly couched can be more than a little inaccessible to "the man in the Clapham omnibus".

Inevitably, data protection compliance is a team effort involving both outward looking ethics and a wide range of skills, not least of which is communication. That is particularly the case in respect of the transparency obligation. Despite this, our overall impression is that almost no organisation represented in the data set seems to have considered this requirement of the GDPR from the perspective of the data subject.

Corporate compliance commonly takes a self referential pragmatic approach on the lines of *"what's the least we need to do to cover ourselves?"* This can in general only address the headlines of a standard or regulation rather than ensuring verified fulfilment of the principles it supports. While such an approach can be sufficient to pass audit for non-statutory requirements such as voluntary certification against public standards, it typically fulfils only the bare minima of genuine compliance. It is not even open to question whether it passes muster for data protection. It does not.

Reassessing risk

Risk under the GDPR is exclusively defined as risk to data subjects and third parties. The Regulation does not consider risk to data controllers, so to achieve compliance the emphasis of corporate governance must be inverted from the conventional inward looking perspective to an outward looking one.

The function of a privacy notice — of *transparency* — is to allow data subjects to identify processing that infringes their rights and freedoms, and to take steps to curtail that infringement. Those rights and freedoms are, officially, a matter of human rights not merely data rights, so the GDPR Chapter III rights are not the sum total of those available to data subjects. They are merely the basis of means whereby data subjects can assure protection of their human rights in respect of personal data processing. Consequently, if a privacy notice fails to serve that purpose, it is by definition non-compliant with the Regulation. Therefore making it difficult or impossible for a data subject to exercise their Chapter III rights is itself a breach of the legislation that leaves an organisation open to challenge and potential penalties.

Although there is no specific right to object to an inadequate privacy notice, the right to lodge a complaint with a supervisory authority is provided for by Article 77, judicial remedy is provided for by Article 79 and compensation by Article 82. Therefore, although the GDPR is silent on data controller risk, the risk arising from failure to satisfy the spirit and purpose as well as the letter of the transparency obligation should be self-evident. It can be minimised by organisations putting themselves conceptually in the data subject's shoes and asking a simple question

"would we as private individuals be satisfied with this privacy notice as sufficient guidance to exercise our data subject rights?"

Acknowledgements

We wish to record our thanks to Peter Barnes of Barnes Meridian consulting for invaluable contributions to the design of this study and helpful discussions as it progressed, and to members of the public whose anonymity we preserve for providing their views on the accessibility and readability of privacy notices.

Annex A

Represented business verticals			
accountants	advertising brokers	book publishers	broadcasters
business services	campaigning	charities	consumer guidance
consumer travel	credit reference agencies	data protection consultants	education providers
energy suppliers	entertainment	event organisers	financial services
government agencies	graphic designers	health care providers	hospitality
HR support	insurance brokers	IT consultancies	journalistic publishers
general legal services	manufacturing	marketing services	online communities
political parties	professional associations	recruitment agencies	retailers
standards bodies	technology vendors	telecoms providers	tourism
trade unions	transportation	web development services	

BiR Business Information Risk Management Consulting
consulting@businessinforisk.co.uk

barnesmeridian
info@barnesmeridian.com