How to Make Privacy Policies both GDPR-Compliant *and* Usable

Karen Renaud
School of Design and Informatics
Abertay University
Dundee, United Kingdom
k.renaud@abertay.ac.uk

Lynsay A. Shepherd
School of Design and Informatics
Abertay University
Dundee, United Kingdom
lynsay.shepherd@abertay.ac.uk

***Abstract*—It is important for organisations to ensure that their privacy policies are General Data Protection Regulation (GDPR) compliant, and this has to be done by the May 2018 deadline. However, it is also important for these policies to be designed with the needs of the human recipient in mind. We carried out an investigation to find out how best to achieve this.**

We commenced by synthesising the GDPR requirements into a checklist-type format. We then derived a list of usability design guidelines for privacy notifications from the research literature. We augmented the recommendations with other findings reported in the research literature, in order to confirm the guidelines. We conclude by providing a usable and GDPR-compliant privacy policy template for the benefit of policy writers.

I. Introduction

Those who surf the web risk having their privacy violated. They need to be informed about what personal data websites are collecting so that they can choose to patronise those who do not violate their privacy, or opt out of the use of their information. In other contexts there is evidence that people do respond to warnings [1], [2], with confirmation from a study in the privacy context [3]. Yet it is non-trivial to design effective privacy policies [4].

Obar and Oeldorf-Hirsch [5] found that 74% of the 543 people in their study did not even read the privacy policy. Where websites force users to read and agree to their policies (e.g. Google), they often become discouraged and overwhelmed because the text is overly long or incomprehensible [6]. Computer users often receive too many privacy advisements [3], [7], [8], and sometimes do not know what actions to take as a consequence of policy information [9].

The Web Content Accessibility Guidelines[1] require notifications to be perceivable, operable, understandable and robust [10]. The evidence from investigations into privacy policy examples suggests that they do not demonstrate these qualities [6]. This diminishes the efficacy of policy notifications, and leaves users vulnerable to unknowingly carrying out actions that will compromise their privacy.

The advent of GDPR adds another level of complexity to the design of privacy policies. Guidance provided by the Information Commissioner's Office [11] stresses the importance of communicating the necessary privacy information to stakeholders, and raising awareness as to the impact of how the organisation implements GDPR requirements. GDPR also requires privacy policies to deliver their message effectively, efficiently and to the user's satisfaction i.e. usably.

Usability methods seek to make policies look less like legal documents, usually worded in legalese, ensuring that the man and woman in the street is able to understand it. Legalese prevents computer users being given fair notice due to poor understandability [12]. Clear and unambiguous communication is, in essence, the *raison dêtre* of privacy policies.

The problem is perhaps that traditional usability guidelines cannot necessarily be used "as-is" in the privacy context because usability testing is usually related to primary task completion. Privacy, on the other hand, is seldom the end user's primary task [13], [14]. That being so, the display of a privacy policies can interrupt the user's pursuit of their primary goal and is thus often perceived to be a nuisance [15]. We need bespoke guidelines to inform policy design in the privacy context.

Waldman [12, p. 8] reports that their review of 191 privacy policies convinced them that "*today's privacy policies are not designed with readability, comprehension, and access in mind*". This justifies the need for explicit usability guidelines to be provided to web privacy policy writers.

Our work seeks to inform policy writers, with guidance that is specifically tailored towards browser-based privacy policies that are both usable and GDPR-compliant.

We first detail the context of our investigations in Section II then summarise the GDPR legislation requirements in Section III. We carried out a systematic literature review of design guidelines for designing usable privacy policies (Section IV). To make our guidelines as helpful as possible, we decided to convey the *spirit* of the guidelines in the form of a privacy policy template. This conveys the "how" of privacy policy design, rather than the "what", as encapsulated in a linear set of policy design guidelines. The paper provides a template pattern for a policy that is both usable and GDPR compliant (Section V), before concluding in Sections VI and VII

[1]https://www.w3.org/TR/WCAG21/

II. Preamble

Wogalter and Mayhorn [16] explain that warnings (policy items) are a type of risk communication. Wogalter [17] explains that warnings have two purposes, to: (1) communicate information, and (2) reduce unwise behaviours. To achieve these aims, the policies have to be designed carefully.

To understand how humans process communications, we need to look at how researchers have modeled this. Wogalter, DeJoy, and Laughery [18] developed the C-HIP model in the context of warning research. Their model builds on initial human communication models proposed by Shannon [19] and Lasswell [20]. Wogalter *et al.*'s model can be considered to be somewhat unrealistic because it does not include a noise component, as Shannon's does. In a world of noisy communication such a model can not be complete. Cranor [21] proposed a human-in-the-loop framework which is more comprehensive and reflects the factors impacting communications in the context of *security* notifications.

It is important to realise that security and privacy are fundamentally different concepts. Skinner *et al.* [22] argue that a secure information system does not necessarily imply that privacy will be preserved in the system. Gritzalis and Lambrinoudakis [23], and Bambauer [24, p. 667] make similar arguments. As an example, they refer to a company that collects customer information and stores it in an encrypted format. This ensures that the information is secured. Yet the same company may sell the information to another company, thereby violating the owner's privacy.

Privacy and security, being clearly distinct concepts, require different models of notification design. This means that we cannot merely use the security communication processing models to inform the design of privacy policies. In the absence of a published privacy communication model, we plan to use the GDPR legislation to structure our privacy policy design guidelines.

III. GDPR Legislation

The introduction of the GDPR is said to be *"the most important change in data privacy regulation in 20 years"* [25]. The legislation will come into force on the 25th May 2018, and replaces the existing Data Protection Directive 95/46/EC. Organisations that fail to comply will be subject to significant fines. The main GDPR requirements are that customers must be informed about (numbering is ours):

GDPR1: Specify Data Being Collected: Customers should be aware of the information that is collected about them. Furthermore, businesses should document the information that is collected, which links into the accountability required by GDPR [11].

GDPR2: Justification For Data Collection: Organisations must explain their rights to collect data [11], but they should also justify to themselves exactly *why* they need to collect such information [26].

GDPR3: How Data Will Be Processed: The organisation must inform the customer of the lawful rights it has to process personal data [11].

GDPR outlines the ways in which processing is deemed legal (one of the following must apply): the customer has given consent for this to be done for a specific purpose, it is used to form a contract with a customer, the data controller is complying with a legal obligation, it is used to protect the interests of a person, it is required for a task involving the public interest, it is required for a legitimate purpose by the controller (provided rights and freedoms are not violated) [27]. Moreover, the person has the right to opt out of processing of his data by an algorithm, or any other profiling.

Under Article 9 of the legislation, there is a special category of data, deemed 'sensitive data' which requires further protection. This information can include details of an individual's health, political views, religion, etc. A lawful basis for processing such information must be given (these have been outlined in a previous paragraph), and a separate basis must be provided for processing special category data [28]. Examples of reasons for processing such data include: it may be necessary for reasons of public health, or it may be necessary for the progression of legal claims [28].

GDPR4: How Long Data Will Be Retained: GDPR dictates that data should be held for the minimum amount of time, and organisations must state how long data is retained [11] [29].

GDPR5: Who Can Be Contacted to Have Data Removed or Produced: People have the right for all their data, both provided to the company, and observed by their systems: (1) to be forgotten, and (2) to be provided to them. To facilitate this, contact details must be provided in the policy [30], [31]. Within the organisation, someone must take responsibility for the stored and processed data. Customers should also be informed who the Data Protection Officer (controller) is, and how to get in touch with them, should they have an access request [11]. Customers should also be provided with a timescale in terms of how subject access requests will be handled by the organisation [11].

GDPR6: Communication of Privacy Information: Documentation on the legislation notes that it "*requires the information to be provided in concise, easy to understand and clear language*" [11].

We now present a GDPR-compliant policy template in Figure 1.

A. Assessing Current State of Play

To take a snapshot of the current situation, roughly three months before the GDPR deadline, we proceeded to assess the privacy policies of some UK-based websites. We carried out this assessment on the 25th January 2018.

In order to choose the UK websites to assess, we consulted Alexa to obtain the top 10 most-used websites in the UK[2].

The **first** step is to be able easily to locate the policy. Langhorne [32] reported, in 2014, that many organisations did not provide a handy link to their privacy policies from the landing page. It is likely that the upcoming GDPR legislation will mandate provision of such links. All of the websites we

[2]https://www.alexa.com/topsites/countries/GB Alexa uses web traffic analysis to produce lists of the most popular websites in countries worldwide

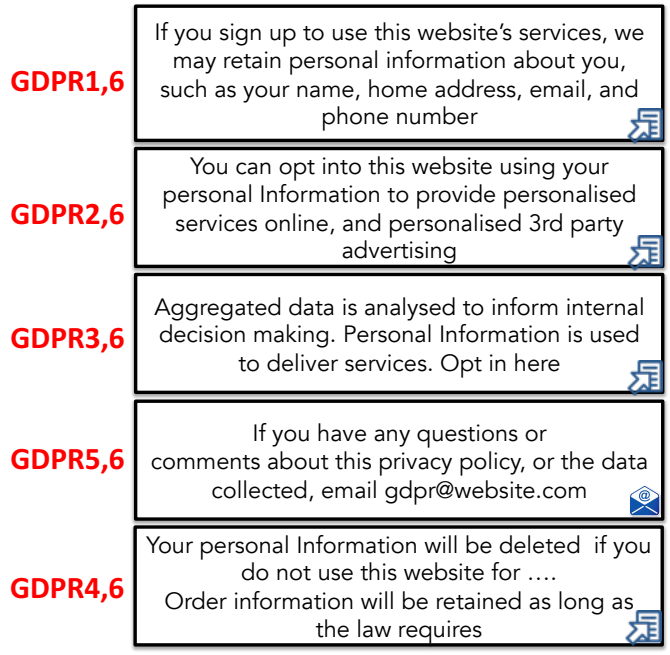

Fig. 1. GDPR-Compliant Policy Template. Each section provides a link to more comprehensive information

examined did indeed include a link to their privacy policy from their main page, which was a positive development.

Secondly, we checked the extent to which the websites' privacy policies satisfied GDPR requirements. To provide a measure of understanding (GDPR6), we use the Gunning Fog Index score[3]. This index is an indication of the number of years of schooling someone would need to be able to understand the text. If someone needs more than a high school education to understand the policy (more than 13 years), we conclude that it fails GDPR6 in terms of understandability. Table I presents our findings.

We also provide the number of words in total, as well as the number of complicated words (with 3 or more syllables) to give an idea of the effort a user would have to expend if they wanted to read and understand the entire policy. The data is depicted in Figure 2.

Only one of these policies met the requirements of the GDPR legislation on the 28th January 2018. There is still time left for the others to revise their policies and they will probably do so, most being large companies with substantial web development resources at their disposal. Yet smaller companies would probably benefit from some guidance in this respect.

In the next section we consider what the research literature says about how to design privacy policies.

IV. Usability Guidelines

We decided to focus on browser privacy policies firstly because of the popularity of web applications [33] such as email, claimed to be the most popular application in use [34]. Video streaming [35], which runs within browsers, is also very popular. The second reason is that browsers run on all devices, ranging from Desktops to Smartphones. We thus felt that our guidelines could be most useful to developers if we focused on guidelines for browser application policy writers.

We carried out a systematic literature review in order to gather best practice from the research literature in this respect.

A. Systematic Literature Review

The literature search was carried out in January 2018 as follows:

Databases: ACM, Springer, Web of Science, Scopus, IEEE, and then Google Scholar to identify publications that did not appear in the databases.

Keywords: 'design guidelines' *and* 'browser'*and* 'privacy' *and* ('feedback' *or* 'warnings' *or* 'notification' *or* 'alert'). A separate search was conducted using the phrase 'privacy policy design'.

Time Range: 2007—2017

Exclusion Criteria: Patents, citations, non-peer reviewed, not English or unobtainable.

[3]http://gunning-fog-index.com/

GDPR Number	1	2	3	4	5	6		
						GFI	Words	3+ Syllable Words
Google.co.uk	●	●	●	⊗	⊗	15.21	2831	487
YouTube	●	●	●	⊗	⊗			
Google.com	●	●	●	⊗	⊗			
Facebook	●	●	●	⊗	⊗	13.71	2697	416
Reddit	●	●	●	⊗	⊗	13.86	2680	423
Amazon.co.uk	●	●	●	⊗	●	12.21	3059	581
BBC*	●	●	●	●	●	11.34	5187	608
Wikipedia	●	●	●	●	⊗	13.74	445	91
eBay	●	●	●	⊗	⊗	**17.97**	5260	994
Twitter	●	●	●	⊗	⊗	13.51	3793	586

TABLE I
Top Alexa Websites and GDPR Requirements. Starred Websites are GDPR Compliant.
(GFI=Gunning Fog Index: ●=satisfies; ⊗=does not satisfy)

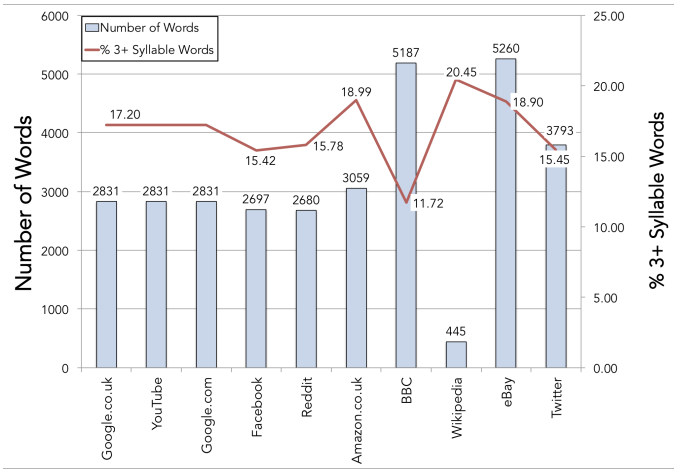

Fig. 2. Word Lengths and % of Complicated Words (3+ syllables)

Database	Returned	Excluded	Analysed
Scopus	0	0	0
ACM	3	2	1
Springer	145	139	6
Web of Science	0	0	0
Google Scholar	61	42	19
IEEE	73	70	3
Total			29

TABLE II
PAPERS FROM THE LITERATURE SEARCH

We analysed the guidelines using Thematic Analysis [36]. This approach supports pinpointing, examining, and recording themes that emerge from the papers. We commenced by familiarising ourselves with the papers. We then generated initial codes and searched for themes as we collated these codes. We then reviewed the themes, defining and naming them. Finally, we assigned them to the applicable GDPR category, as detailed in Section III.

B. Results

GDPR1*:* Ensure that the sensitivity of the data is communicated to the user [37]. This need is confirmed by [38].

GDPR2*:* Some researchers advise that providing justifications for privacy policies potentially reduces the end-user's trust in the system [39], [40], [41], [42]. Volkamer *et al.* [43] advise that the potential consequences of a risk be conveyed to the user, along with potential recommendations. GDPR mandates that this information be provided so we should focus on fostering trust in the presence of such justifications.

GDPR3*:* —

GDPR4*:* —

GDPR5*:* It is important to ensure that the user can contact someone in the organisation [44], [45]. Contact details should be conspicuously placed [46].

GDPR6*:* In this section we first present the themes that emerged from our analysis. We then cite supporting research from other publications. The themes fell naturally into two meta categories: (1) content of the policies, and (2) delivery of the policies. We report these separately

Content Guidelines:

The overarching admonition should be that human attention is a finite resource [47], [45] that should not be taken for granted or squandered, and privacy policies *"should empower users to make informed decisions about their online behavior"* [48].

(a) Modality — Murphy-Hill & Murphy [49], [50] suggest that pictures be used to ease communication because users prefer this [51]. Others have advocated visualising privacy policy statements, making them more usable [45].

On the other hand, Goldberg [44] suggests that text should be used exclusively to maximise accessibility. Anderson *et al.* [52], [53] suggests the use of polymorphism in warning notifications to reduce habituation.

Supporting Research: Other researchers argue for the power of a multi-modality image and text message in enhancing communication [54], [55], [56], [57].

(b) Make it Personal — Vasalou [58] says policy items should give recipients "space for interpretation", so that they can understand how it applies particularly to them [59]. The personalisation of policies should be considered [51], [60], [61], [62]. .

Supporting Research: Elman *et al.* [63] argue that personalisation, by whatever means, is extremely important in enhancing understanding. Schaub *et al.* [64] says privacy policy notices should be "relevant" to the person. Needham [65] also argues for the importance of personalisation. Yet policy display is somewhat different from other kinds of personalisation opportunities: people view the policy *before* they have divulged any information that could be used to personalise the communication. That being so, one way of personalising a generic document, such as a policy, especially in helping people to see that it applies to them, could be by using personal pronouns like "you" and "your". This should help people to consider the personal ramifications of the policy.

Another way is to provide examples that people can identify with [66], but this will take up valuable space and needs detailed investigation to assess viability.

(c) Give Control to the User — It is important for the user to retain a level of control [46], [58], [67] by allowing them to exercise control over disclosure [47]. Schaub *et al.* [68] distinguish between three levels of user control: (1) blocking, non-blocking and decoupled. A designer has to decide whether the user has to acknowledge the policy notification (blocking) or not (non-blocking), whether they can defer their response (decoupled), or whether the option's actions will expire [49].

Users should be provided with the option to respond to a risk they have been notified about, and helped to visualise potential consequences [60], [69].

Supporting Research: Other research emphasises the need to allow people to control disclosure [38], [64]. Yet Waldman [12] reports that, of the 191 policies they surveyed in 2016, only 9 provided users with noticeable opt-out buttons. Moreover, they discovered that a little more than half of these only allowed users to opt out of marketing, but not out of profiling. GDPR mandates that users should be allow to opt out of the latter. Yet Adjerid *et al.* [70] point out that merely allowing people to opt out, without carefully considering the way the information about such consent is presented to the user is framed, does not necessarily help them to make better privacy choices.

(d) Trust — Trust should be deliberately built and maintained [49], [12] by framing the privacy policy very carefully [40]. Indeed, when people read privacy policies, it impacts on their trust of the website [71], so it is important to get it right.

It is crucial for people to trust a website if they are to make use of it [72]. Broutsou and Fitsilis [73] review the literature on trust and report a number of studies that show that the level of trust is positively related to the intention to carry out an online transaction.

Supporting Research: Other research suggests that users require reassurance that information is kept securely [38], [45] and recommend including a Privacy Seal [74], [30],

[31], [72]. Policy writers should also provide a telephone number (not only an email address) and make other channels of communication clear [30], [31]. Finally, the policy should explain how these privacy assurances will be enforced [75], [76].

(e) Overview & Link — Lin [59] suggests highlighting the most important information. We should only present essential details about the risk [60], [61], with links to more information should they want it [43]. In providing policy-based notifications, a balance must be found between brevity and comprehensiveness [13].

Supporting Research: Researchers confirm the need to provide an overview first and then links to more information [31], [74]

(f) Maximise Understandability — This is emphasised by a number of researchers [14], [49], [50], [77], [69], [78], [12] as well as the importance of consistency [10], [49].

Unclear notifications are more likely to be ignored, and consideration should be given to the exact meanings of words used [60]. Concrete explanations should be provided [79], [80] and explanations should be simple [59], avoiding acronyms and jargon with only meaningful terminology being used [13], [14], [77], [2]. Semantically distinct information should be separated [14], [58]. Text should be presented in short, simple sentences, devoid of complex grammatical structures [81], [82], [83], [84]. Longer warning notifications performed poorly in user testing [85].

Some users may have low numeracy levels so that other mechanisms for communicating risk should be sought. In choosing these, it should be borne in mind that users may have different understanding of visuals [60].

Supporting Research: Other authors confirm the importance of maximising ease of use [72], [86], [64].

In terms of understandability, it must be noted that existing work confirms that shorter notifications are most effective at communicating with users. The challenge, in providing enough information to foster understanding, while being brief, is highlighted [87].

Delivery Guidelines:

(i) Timing & Location — Many of the recommendations that fall into this category are related to the delivery of pop-up type alerts and notifications, both in terms of time and space. There is a focus on displaying these only when they merit interrupting the user's task [50], [88], avoid irritating [43] and preventing habituation [49], [88]. Privacy policies, unlike these kinds of alerts, are either viewed when the person deliberately clicks on a link, or is forced to read the policy and consent to it. Hence time and space are less applicable in this context.

(iii) Appearance — Kelley [14] provides a number of recommendations: (1) the notification should be surrounded by a box to clearly demarcate it; (2) provide a title to assist speedy recognition. It is important to be careful with colour use so as not to disadvantage those with colour deficiencies [44]. A neutral grey colour can be used for the background of notifications, as it is unlikely to annoy the user [43].

C. Reprise

It is clear from the previous discussion that much attention has been given to guidelines to ensure that GDPR6 is satisfied. GDPR3 and GDPR4 requirements were not addressed in the literature we gathered, while GDPR1 and GDPR5 did not receive much attention. GDPR2 is an area ripe for focused attention, because many of the current guidelines conflict with the GDPR requirements.

We could simply provide the list of content-related guidelines based on the derived principles in the previous section. However designers have difficulty benefiting from these kinds of flat lists of guidelines [89], [90]. We therefore plan to produce a template to demonstrate the impact of these guidelines. Waldman [12] discovered that a demarcated structure for policies made them more palatable to users.

V. Usable and GDPR-Compliant Privacy Policy Template

In this section we consider how to implement the content guidelines from the literature as described in the previous section. The delivery guidelines will not be considered because they have a great deal to do with the context and nature of the website and cannot be provided in a context-neutral fashion.

In providing an example GDPR-compliant template, we formulated text to deliver the content for a fictional Company X, as advised by the GDPR requirements and content guidelines. We measured the understadability of the text by using the Gunning Fog Index test.

Some of the content guidelines are relatively easy to satisfy, more or less in a binary fashion i.e. overview & link. Guidelines (d) (trust) and (f) understandability, require a more nuanced approach.

GDPR6(d) Trust: To address trust issues we decided to include an image to foster and inspire trust. We decided to propose the use of a Privacy Seal for this purpose, especially since this has been widely advised [74], [30], [31], [72]. Moreover, we shall include icons in each subsection to demarcate them and improve accessibility.

GDPR6(f) Maximise Understandability: To maximise the understandability required by GDPR6, we simplified the text to need less than a high school education to understand, and included a small icon to bookmark different sections.

The years of compulsory schooling a person receives depends on the country they are from. For example, in the UK, children attend school from the ages of 5 to 18, however they are free to leave at the age of 16, meaning they can receive between 11 and 13 years of schooling. In contrast, when considering other EU countries, Swedish children start school at the age of 7, and can leave at 16, meaning they may only receive 9 years of schooling.

Research presented in this paper was conducted by an English-speaking, UK-based institution, therefore the assumption was made that people typically have between 11 and 13

years of schooling. Table III provides the GFI of the text provided to address all the GDPR requirements as understandably as possible.

Guideline	GFI	Text Used
GDPR1	8.457	If **you** sign up to use this website's services, we may keep personal information about **you**. This will include **your** name, home address, email, and phone number
GDPR2, GDPR6(c)	6.105	We would like to use your information to provide better services to you, and adverts from 3rd parties. Opt in here
GDPR3	5.822	We would like to collect all order information to help us to predict global trends. Opt in here
GDPR4	11.47	Order information is kept to meet legal requirements. **Your** personal Information will be deleted if you do not use this website for a month
GDPR5	11.40	If **you** have any questions or comments about this privacy policy, or the data collected, email ...
GDPR6(d)	11.67	**Your** data is stored safely and securely. If we do lose **your** data we will be fined by the Information Commissioner

TABLE III
TEMPLATE TEXT GUNNING FOG INDEX

An exemplar GDPR-compliant and usable privacy policy was derived from the template shown in Figure 1 and is shown in Figure 3. Company X, the company this privacy policy was tailored for, only uses their customers' information to detect global trends, and this is reflected in the middle box. This box, in particular, would reflect the purposes any particular organisation intends to use the customer's data for. The box on the right would also reflect a specific company's deletion policy; Company X only keeps data for 1 month — others may keep it for 2 years. It is important that the actual policy is reflected here, so that the policy satisfies GDPR requirements.

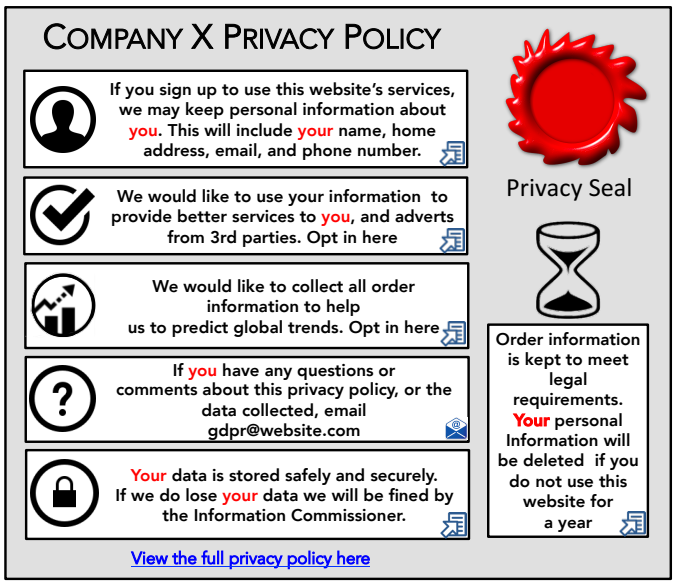

Fig. 3. Usable GDPR-Compliant Privacy Policy Example

VI. FUTURE WORK

The incoming GDPR legislation requires websites to obtain consent from their customers/users for any data collection to take place. This will inevitably lead to a veritable avalanche of consent requests as the GDPR deadline approaches. It is possible, as Schermer *et al.* [91] argue, that people will become desensitised by all these requests and will start consenting without being fully aware of what they are consenting to. Adjerid *et al.* [40] also argue that a myopic focus on transparency enhancement will not necessarily lead to improved and informed consent, especially when sites frame information differently. It would be very interesting to explore these apparent conundrums.

We proposed the use of a privacy seal to foster trust. A more detailed investigation is required in order to determine whether this is the most effective image to use. Some researchers found that privacy seals did enhance trust [92] but there is also evidence that users often misinterpret their message [93].

VII. CONCLUSION

We publish this work to provide guidance to designers and developers who need to incorporate privacy policies into their systems. Our final template draws on the GDPR legislation and the research literature on usable design. We welcome feedback, particularly from those working in industry, to help us to refine and improve this template, to help it deliver maximum value.

ACKNOWLEDGEMENTS

We thank Andrew Phillips for his feedback on an earlier draft of this paper.

REFERENCES

[1] E. P. Cox III, M. S. Wogalter, S. L. Stokes, and E. J. Tipton Murff, "Do product warnings increase safe behavior? A meta-analysis," *Journal of Public Policy & Marketing*, pp. 195–204, 1997.

[2] M. Silic, J. Barlow, and D. Ormond, "Warning! A comprehensive model of the effects of digital information security warning messages," in *The 2015 Dewald Roode Workshop on Information Systems Security Research*. IFIP, 2015.

[3] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 1065–1074.

[4] R. LaRose and N. J. Rifon, "Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 127–149, 2007.

[5] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," in *TPRC 44: The 44th Research Conference on Communication, Information and Internet Policy*, 2016.

[6] J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. McDonald, T. B. Norton, and R. Ramanath, "Disagreeable privacy policies: Mismatches between meaning and users' understanding," *Berkeley Tech. LJ*, vol. 30, p. 39, 2015.

[7] S. Kim and M. S. Wogalter, "Habituation, dishabituation, and recovery effects in visual warnings," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 53, no. 20. Sage Publications Sage CA: Los Angeles, CA, 2009, pp. 1612–1616.

[8] B. Anderson, T. Vance, B. Kirwan, D. Eargle, and S. Howard, "Users aren't (necessarily) lazy: using neuroIS to explain habituation to security warnings," in *Thirty Fifth International Conference on Information Systems*, Auckland, 2014.

[9] U. Shankar and C. Karlof, "Doppelganger: Better browser privacy without the bother," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*. ACM, 2006, pp. 154–167.

[10] L. D. A. Almeida and M. C. C. Baranauskas, "Merging technical guidelines for accessible web content with universal design principles," Tech. Rep. IC-10-020, 2010.

[11] Information Commissioner's Office, "Preparing for the General Data Protection Regulation (GDPR) - 12 Steps to Take Now," 2018, https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

[12] A. E. Waldman, "Privacy, Notice and Design," 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2780305.

[13] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brother's watching you: Raising awareness of data leaks on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 12.

[14] P. G. Kelley, "Designing a privacy label: assisting consumer understanding of online privacy practices," in *CHI'09 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2009, pp. 3347–3352.

[15] E. Albrechtsen, "A qualitative study of users' view on information security," *Computers & Security*, vol. 26, no. 4, pp. 276–289, 2007.

[16] M. Wogalter and C. Mayhorn, "Warning design," in *Information Design: Research and Practice*, A. Black, P. Luna, O. Lund, and S. Walker, Eds., 2017, ch. 20.

[17] M. S. Wogalter, "Factors Influencing the Effectiveness of Warnings," *Visual Information for Everyday Use: Design and Research Perspectives*, pp. 93–110, 1999.

[18] M. S. Wogalter, D. M. DeJoy, and K. R. Laughery, "Organizing theoretical framework: a consolidated communication-human information processing (c-hip) model," *Warnings and Risk Communication*, pp. 15–23, 1999.

[19] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.

[20] H. D. Lasswell, "The Structure and Function of Communication in Society," *The Communication of Ideas*, vol. 37, pp. 215–228, 1948.

[21] L. F. Cranor, "A framework for reasoning about the human in the loop." *UPSEC*, vol. 8, no. 2008, pp. 1–15, 2008.

[22] G. Skinner, S. Han, and E. Chang, "A framework of privacy shield in organizational information systems," in *International Conference on Mobile Business. (ICMB 2005)*. IEEE, 2005, pp. 647–650.

[23] S. Gritzalis and C. Lambrinoudakis, "Privacy in the digital world," in *Encyclopedia of Internet Technologies and Applications*. IGI Global, 2008, pp. 411–417.

[24] D. E. Bambauer, "Privacy versus Security," *J. Crim. L. & Criminology*, vol. 103, p. 667, 2013.

[25] EU Parliament, "Home Page of EU GDPR," 2018. [Online]. Available: https://www.eugdpr.org/

[26] A. Cormack, "GDPR: What's your justification?" 2017, https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification,journal=JISC Community.

[27] Intersoft Consulting, "Art. 6 GDPR Lawfulness of processing," 2016, https://gdpr-info.eu/art-6-gdpr/.

[28] I. C. Office, "Special Category Data," 2018, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/?q=best+practice,journal=Information Commissioner's Office.

[29] Data Protection Network, "GDPR Data Retention Quick Guide," 2017, https://www.dpnetwork.org.uk/gdpr-data-retention-guide/.

[30] P. Durkan, M. Durkin, and J. Gillen, "Exploring efforts to engender on-line trust," *International Journal of Entrepreneurial Behavior & Research*, vol. 9, no. 3, pp. 93–110, 2003.

[31] J. Gantner, L. Demetz, and R. Maier, "All you need is trust–an analysis of trust measures communicated by cloud providers," in *OTM Confederated International Conferences. On the Move to Meaningful Internet Systems*. Springer, 2015, pp. 557–574.

[32] A. L. Langhorne, "Web privacy policies in higher education: How are content and design used to provide notice (or a lack thereof) to users?" in *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2014, pp. 422–432.

[33] M. S. Mikowski and J. C. Powell, *Single Page Web Applications*. Manning Publications, 2013.

[34] S. Alharbi and D. Rigas, "Graphical browsing of email data: An empirical investigation," in *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on*. IEEE, 2008, pp. 495–499.

[35] A. Kellerman, "Mobile broadband services and the availability of instant access to cyberspace," *Environment and Planning A*, vol. 42, no. 12, pp. 2990–3005, 2010.

[36] G. Guest, N. MacQueen, and E. Namey, "Introduction to thematic analysis," *Applied Thematic Analysis*, vol. 12, 2012.

[37] S. Nafra, "Aligning privacy and usability: Designing a privacy-aware mobile application that people can use," Master's thesis, Vienna University of Economics and Business, 2014.

[38] C. Liu, J. T. Marchewka, J. Lu, and C.-S. Yu, "Beyond concerna privacy-trust-behavioral intention model of electronic commerce," *Information & Management*, vol. 42, no. 2, pp. 289–304, 2005.

[39] M. Aagaard, "How Privacy Policy Affects Sign-Ups — Surprising Data From 4 A/B Tests," *ContentVerve. com*, 2013.

[40] I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein, "Sleights of privacy: Framing, disclosures, and the limits of transparency," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 9.

[41] B. P. Knijnenburg, "A user-tailored approach to privacy decision support," Ph.D. dissertation, Information and Computer Sciences, 2015.

[42] I. Pollach, "What's wrong with online privacy policies?" *Communications of the ACM*, vol. 50, no. 9, pp. 103–108, 2007.

[43] M. Volkamer, K. Renaud, G. Canova, B. Reinheimer, and K. Braun, "Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness," in *Trust and Trustworthy Computing - 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings*, 2015, pp. 104–122.

[44] J. S. Goldberg, "State of Texas Municipal Web Sites: A Description of Website Attributes and Features of Municipalities with Populations Between 50,000-125,000," Master's thesis, Public Administration, 2009.

[45] T. Albalawi and K. Ghazinour, "A usability study on the privacy policy visualization model," in *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, DASC/PiCom/DataCom/CyberSciTech 2016, Auckland, New Zealand, August 8-12, 2016*, 2016, pp. 578–585. [Online]. Available: https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.109

[46] John Sören Petterson (Ed.), "HCI Guidelines," 2008, PRIME (Privacy and Identity Management for Europe) EU Project Report.

[47] J. H. Colnago, "Privacy agents in the IoT: considerations on how to balance agent autonomy and user control in privacy decisions," Ph.D. dissertation, Universidade Federal de São Carlos, 2016.

[48] A. L. Langhorne, "Web privacy policies in higher education: How are content and design used to provide notice (or a lack thereof) to users?" in *Human Aspects of Information Security, Privacy, and Trust - Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings*, 2014, pp. 422–432. [Online]. Available: https://doi.org/10.1007/978-3-319-07620-1_37

[49] E. Murphy-Hill and G. C. Murphy, "Recommendation delivery," in *Recommendation Systems in Software Engineering*. Springer, 2014, pp. 223–242.

[50] T. Westermann, "User acceptance of mobile notifications," Ph.D. dissertation, Institute of Software Engineering and Theoretical Computer Science, Berlin Institute of Technology Berlin, Germany, 2017.

[51] Y. Chen, F. Zahedi, and A. Abbasi, "Interface design elements for anti-phishing systems," in *Proceedings of the 6th International Conference on Service-oriented Perspectives in Design Science Research*, ser. DESRIST'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 253–265.

[52] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance, "How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2883–2892.

[53] B. B. Anderson, A. Vance, C. B. Kirwan, J. L. Jenkins, and D. Eargle, "From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it," *Journal of Management Information Systems*, vol. 33, no. 3, pp. 713–743, 2016.

[54] F. P. Karimov, M. Brengman, and L. Van Hove, "The effect of website design dimensions on initial trust: a synthesis of the empirical literature," *Journal of Electronic Commerce Research*, vol. 12, no. 4, p. 272, 2011.

[55] R. Merchant, "What local consumers want most from local business websites," https://www.brightlocal.com/2014/02/06/what-local-consumers-want-most-from-local-business-websites/ April 11, 2017 (Accessed 31/1/18).

[56] P. Messaris, *Visual persuasion: The role of images in advertising*. Sage, 1997.

[57] P. Messaris and L. Abraham, "The role of images in framing news stories," *Framing public life: Perspectives on Media and our Understanding of the Social World*, pp. 215–226, 2001.

[58] A. Vasalou, A.-M. Oostveen, C. Bowers, and R. Beale, "Understanding engagement with the privacy domain through design research," *Journal of the Association for Information Science and Technology*, vol. 66, no. 6, pp. 1263–1273, 2015.

[59] J. Lin, "Understanding and capturing people's mobile app privacy preferences," Ph.D. dissertation, Carnegie Mellon University, 2013.

[60] J. R. Nurse, "Effective communication of cyber security risks," in *7th International Scientific Conference on Security and Protection of Information (SPI 2013)*, 2013.

[61] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in *The 3rd International Workshop on Cyberspace Safety and Security (CSS 2011) at The 5th International Conference on Network and System Security (NSS 2011)*. IEEE, 2011.

[62] E. M. Redmiles, E. Liu, and M. L. Mazurek, "You Want Me To Do What? A Design Study of Two-Factor Authentication Messages," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, 2017.

[63] R. J. Elman, J. Ogar, and S. H. Elman, "Aphasia: Awareness, advocacy, and activism," *Aphasiology*, vol. 14, no. 5-6, pp. 455–459, 2000.

[64] F. Schaub, R. Balebako, and L. F. Cranor, "Designing effective privacy notices and controls," *IEEE Internet Computing*, 2017.

[65] C. Needham, *Personalising public services: Understanding the personalisation narrative*. Policy Press, 2011.

[66] C. Robinson and J. Sebba, "Personalising learning through the use of technology," *Computers & Education*, vol. 54, no. 3, pp. 767–775, 2010.

[67] H. Xu, R. E. Crossler, and F. BéLanger, "A value sensitive design investigation of privacy enhancing tools in web browsers," *Decision Support Systems*, vol. 54, no. 1, pp. 424–433, 2012.

[68] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, 2015, pp. 1–17.

[69] R. Jones, N. Sailaja, and L. Kerlin, "Probing the design space of usable privacy policies: A qualitative exploration of a reimagined privacy policy," in *Proceedings BHCI*, 2017.

[70] I. Adjerid, A. Acquisti, and G. Loewenstein, "Framing and the malleability of privacy choices," in *Proceedings of the 13th Workshop on the Economics of Information Security*, 2014.

[71] K. Martin, "Formal versus informal privacy contracts: Comparing the impact of privacy notices and norms on consumer trust online." 2015, https://www.law.uchicago.edu/files/file/martin_formal_versus_informal_privacy_contracts.pdf.

[72] S. Sun, T. Wang, L. Chen, and M. Wang, "Understanding Consumers' Trust in Internet Financial Sales Platform: Evidence from "Yuebao"," in *PACIS*, 2014, p. 199.

[73] A. Broutsou and P. Fitsilis, "Online trust in the greek context: The influence of perceived companys reputation on consumers trust and the effects of trust on intention for online transactions," in *the Proceedings of the Management of International Business and Economic Systems (MIBES-ESDO) 2012 International Conference, School of Management and Economics, TEI of Larissa, Greece*, 2012.

[74] J. Johnston, J. H. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, vol. 22, no. 8, pp. 675–684, 2003.

[75] K.-W. Wu, S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust," *Computers in Human Behavior*, vol. 28, no. 3, pp. 889–897, 2012.

[76] N. Doty and M. Gupta, "Privacy design patterns and anti-patterns," in *Trustbusters Workshop at the Symposium on Usable Privacy and Security*, 2013.

[77] R. Shah and K. Patil, "Evaluating effectiveness of mobile browser security warnings," *ICTACT Journal on Communication Technology*, vol. 7, no. 3, pp. 1373–1378, 2016.

[78] S. Kununka, N. Mehandjiev, P. Sampaio, and K. Vassilopoulou, "End User Comprehension of Privacy Policy Representations," in *International Symposium on End User Development*. Springer, 2017, pp. 135–149.

[79] A. A. Ozok, Q. Fan, and A. F. Norcio, "Design guidelines for effective recommender system interfaces based on a usability criteria conceptual model: results from a college student population," *Behaviour & Information Technology*, vol. 29, no. 1, pp. 57–83, 2010.

[80] A. W. Y. Ng and A. H. S. Chan, "Mental Models of Construction Workers for Safety-Sign Representation," *Journal of Construction Engineering Management*, vol. 143, no. 2, 2017.

[81] M. Harbach, S. Fahl, P. Yakovleva, and M. Smith, "Sorry, I Don't Get It: An Analysis of Warning Message Texts," in *Proceedings of the 2013 International Conference on Financial Cryptography and Data Security (FC13), Workshop on Usable Security*, ser. Lecture Notes in Computer Science, 2013.

[82] M. Harbach, S. Fahl, T. Muders, and M. Smith, "Towards measuring warning readability," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, ser. CCS '12. New York, NY, USA: ACM, 2012, pp. 989–991. [Online]. Available: http://doi.acm.org/10.1145/2382196.2382301

[83] M. Pala and Y. Wang, "On the usability of user interfaces for secure website authentication in browsers," in *Proceedings of the 6th European Conference on Public Key Infrastructures, Services and Applications*, ser. EuroPKI'09. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 239–254.

[84] X. Dong, J. A. Clark, and J. L. Jacob, "Defending the weakest link: phishing websites detection by analysing user behaviours," *Telecommunication Systems*, vol. 45, no. 2-3, pp. 215–226, 2010.

[85] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, S. Komanduri, and M. Sleeper, "Improving computer security dialogs," in *Human-Computer Interaction - INTERACT 2011 -13th IFIP TC 13 International Conference, Lisbon, Portugal, September 5-9, 2011, Proceedings, Part IV*, 2011, pp. 18–35.

[86] S. D'Hertefelt, "Trust and the perception of security," 2000, 3 January http://users.skynet.be/fa250900/research/report20000103shd.htm Accessed 30/1/2018.

[87] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving SSL Warnings: Comprehension and Adherence," in *Proceedings of the Conference on Human Factors and Computing Systems*, 2015.

[88] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness." in *USENIX Security Symposium*, vol. 13, 2013.

[89] K. Renaud and J. van Biljon, "Demarcating Mobile Phone Interface Design Guidelines to Expedite Selection ," *South African Computing Journal*, vol. 29, no. 3, 2017.

[90] E. Luger and T. Rodden, "The value of consent: Discussions with designers of ubiquitous computing systems," in *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. IEEE, 2014, pp. 388–393.

[91] B. W. Schermer, B. Custers, and S. van der Hof, "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection," *Ethics and Information Technology*, vol. 16, no. 2, pp. 171–182, 2014.

[92] N. J. Rifon, R. LaRose, and S. Choi, "Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures," *Journal of Consumer Affairs*, vol. 39, no. 2, pp. 339–362, 2005.

[93] R. LaRose and N. Rifon, "Your privacy is assured-of being disturbed: websites with and without privacy seals," *New Media & Society*, vol. 8, no. 6, pp. 1009–1029, 2006.