Privacy: was it Shielded?

Research into a sample of Privacy Shield participants' websites, to establish their compliance with specific aspects of GDPR

DataRep

Summary results

Privacy notice is available on website

90.9% - Privacy notice one click from home screen

5.5% - Privacy notice two clicks from home screen

1.8% - No privacy notice or cookie notice only

1.8% - Privacy notice only available from Privacy Shield website link or cookie banner

Obtaining adequate consent for cookie use

40.1% - Site uses cookies, no consent sought

38.6% - Site uses cookies, notified or consent sought in uncompliant manner

18.2% - Site uses cookies, consent sought in compliant manner

3.1% - Site doesn't use cookies

EU establishment or appointment of Representative

60.2% - Have no EU establishment and have not appointed an EU Representative

34.9% - Have EU establishment

4.9% - Have no EU establishment and have appointed an EU Representative

Please be aware that the results of this survey have a 5% margin of error

DataRep

Contents

Introduction

Privacy Shield had been in use as a GDPR-compliant mechanism by which EU personal data may be transferred to the US since 2016. Before that time, its predecessor Safe Harbour provided this mechanism but, following a 2015 decision by the European Court of Justice (ECJ) – that Safe Harbour failed to provide sufficient protection of EU personal data – Privacy Shield was agreed between the EU and USA to take its place.

Recently, the ECJ found in the Schrems II case that Privacy Shield fails to provide sufficient protection to EU personal data when transferred to the USA, and accordingly it is no longer deemed a GDPR-compliant cross-border personal data transfer mechanism.

The main reasons for the decision were not solely related to the transfer (i.e. the data in motion), but the protections provided to the personal data on its arrival in the USA (the data at rest), where a wide entitlement on the part of the US surveillance authorities to demand access to that data was deemed incompatible with the GDPR requirement that personal data not be shared with those authorities except for the most compelling reasons.

The court also declared that the standard contractual clauses (SCCs) which may be used as an alternative transfer mechanism would only be permitted for EU-to-US transfers where there were additional safeguards to protect that data once it reaches the USA. Although it remains unclear what those safeguards are expected to include, it is apparent that – even with additional safeguards – being a participant of Privacy Shield is not necessarily confirmation that a company is capable of processing EU personal data in a manner compliant with GDPR.

This has come as something of a surprise to businesses which have been sending EU personal data to Privacy Shield participants, apparently comfortable in the knowledge that they are making a compliant transfer to a company which can be trusted to process that personal data so as to not place that transferring company in breach of their own GDPR obligations.

Privacy Shield has been invalidated – but how accurate was the implied compliance with GDPR which it conferred on its participants?

This research

This research was undertaken with the purpose of establishing the extent to which the publicly-accessible websites of a sample of Privacy Shield participants comply visibly with three areas covered by GDPR in the EU, specifically the availability of a privacy notice (Article 13), the extent to which consent has been adequately obtained to process personal data using cookies (Article 6), and whether – if the company has no EU establishment – they have appointed an EU Representative (Article 27). A full explanation of the methodology, and the factors which informed the results, are set out at the end of this document.

We ask the reader to note that this review did not aim to discover whether those Privacy Shield participants considered are fully compliant with GDPR, as the majority of the operational actions required to achieve such compliance occur behind the scenes, so that it would never be possible to confirm whether a data controller or data processor was fully compliant with GDPR without an on-site audit.

Having skimmed the privacy notices, it should be noted that there is a likelihood that there are failings within a number of those documents as well, but further investigation would be needed to assess the extent to which that is the case (and such investigations may be difficult without a deeper understanding of the participant's data processing activities).

It is also worth noting that – despite it being a logical inference – at no point does the Privacy Shield process expressly indicate that participation of a US-based company equates to GDPR compliance. However, because the explicit purpose of the Privacy Shield is a mechanism by which companies may transfer EU personal data in a GDPR-compliant manner, it has been presumed by many of the companies at the EU-end of that transfer that Privacy Shield participation are likely to expect that to be the case, and accordingly this research assumes that a company which has observed the process to join the Privacy Shield will also need to be processing the EU personal data they receive in a manner compliant with GDPR, or a transfer of EU personal data to that company would not be a valid transfer. To summarise, we consider it an impossible conflict for a company to both participate successfully in the Privacy Shield and not be compliant with GDPR.

The purpose of this research is not to "name and shame"; we will not be publishing details of the 384 companies (around 7.3% of the 5,248 listed at the start of the research) whose websites and Privacy Shield website entries have been considered as part of this process. However, following the Schrems II decision, we wanted to establish the extent to which Privacy Shield should previously have given reassurance as to the GDPR compliance of the companies to which were certified by this mechanism – and to use the findings to make recommendations to improve the next iteration of Privacy Shield.

Although it is impossible to assess from the outside whether a company is fully GDPR-compliant, some elements of GDPR compliance (or not) can often be determined from an inspection of the information a company makes publicly available.

For the purposes of this research:

- It is assumed that a company which participates in Privacy Shield is (or expects to be) receiving the personal data of data subjects within the scope of the GDPR.
- It is assumed that a company which participates in Privacy Shield either (a) has an establishment in the EU from which that data is transferred to their US entities or (b) is targeting sales in the EU or monitoring people there.
- Following the two assumptions above, it is assumed that a company which participates in Privacy Shield should be processing the personal data of EU-based individuals in line with the requirements of GDPR, and that a company's participation in Privacy Shield entitles other companies (which are seeking to transfer EU personal data to the participant) to expect that such personal data will be protected in the same manner as it would be in the EU.
- Cookie consents have only been considered against the consent requirements of GDPR and not the more-detailed stipulations around the use of cookies in the ePrivacy Directive or other relevant directives and regulations.

The purpose here is to identify areas of non-compliance which can be quickly and visibly identified from the information provided (or omitted) on the participant's public-facing website and their entry on the Privacy Shield website.

Executive summary

"I hope you find this research – and the recommendations which arose from it – useful and informative, and I invite you to contact me if you have any questions."

Tim Bell, Managing Director of DataRep
timbell@datarep.com

The flow of data has grown in importance over the last few decades, as personal data has become ever-more important to the activities of businesses globally. One of the declared purposes of GDPR was to ensure that personal data was protected, wherever it may be processed – even outside of the traditional jurisdiction of the EU; to nowhere is this more relevant than the USA, the most-frequent location of the companies undertaking personal data processing.

During the operation of Privacy Shield, many companies in the EU have been comfortable to assume GDPR compliance on the part of its participants, as those companies are using a mechanism created to confirm that the recipient provides suitable protections for the EU personal data they receive. After all, if a company is certified by a system which permits transfers of personal data under GDPR, it doesn't take much of a leap to expect that the continued processing of that data will remain GDPR compliant once it arrives in the US (whether simply for storage or more), otherwise what purpose was there in certifying its transfer?

Although the Schrems II judgement has struck down the validity of Privacy Shield (noting that the US Department of Commerce continues to administer the scheme, and accept new participants), it will undoubtedly be replaced with another mechanism. That scheme will presumably provide more safeguards, but I believe the Privacy Shield should (and was assumed to) have always met its implied effect of providing reassurance as to the GDPR compliance of those companies it certified. We carried out this research to discover whether that assumption/implication might be inaccurate.

The results, set out in this document, were certainly disappointing but – in the same way as Privacy Shield being found insufficient by the ECJ – will probably not surprise most who work in data privacy and compliance.

> *There is good news with regard to the existence of a privacy notice, with most (96.4%) companies making this easily available on their website, but compliance with cookie consent under GDPR (21.4%), and appointment of an EU Representative by non-EU companies (6.6%) was disappointing, to say the least.*

It could be argued that the focus of the US end of Privacy Shield is different from that at the EU end. From Europe, the attention is generally on the protection of the privacy rights of EU data subjects, with the need to transact EU-US business as an important – but secondary – aspect; whereas the USA side, represented by the Federal Trade Commission, is dedicated to ensuring the protection of US-based businesses. This focus can be seen with the attention paid by Privacy Shield to US-based arbitration methods as redress for GDPR breaches, presumably with the hope of avoiding costly class actions against US companies, but offering little benefit to EU data subjects who already have the benefit of a rigorous protection and enforcement regime within the EU. I would prefer to see more attention paid to the protection of data subjects' rights, than adding new enforcement methods when those rights are breached – and I believe the often-quoted approach that "it is easier to seek forgiveness than permission" is at odds with the expectation of privacy by design and default which GDPR requires.

Comments on the EU Representative role

Comments about EU establishments or the appointment of EU Representatives by Privacy Shield participants

As a provider of the EU Representative service to our non-EU clients under Article 27 of GDPR, DataRep's interest was naturally drawn to this aspect of the research.

Privacy Shield makes no mention of the EU Representative obligation, which we've always considered odd; this appointment is one of the key benefits added to GDPR to assist cross-border enforcement of rights against non-EU companies. It appears self-evident that the Privacy Shield principles of 'Recourse, Enforcement and Liability' and particularly 'Access' would be better-served where an EU data subject is able to raise their requests within the EU, rather than entering into arbitration in the US.

Although not a specific requirement of GDPR, we interpret the expectation that most data controllers / processors under GDPR have an EU establishment or appoint an EU Representative[1] as an indication that the EU expects companies impacted by GDPR to have an EU address to which requests can be raised, unless there is a specific exclusion from the Representative obligation (usually the only relevant exclusion is "occasional processing"[2], but we anticipate that exclusion would rarely apply to a company which processes sufficient EU personal data to necessitate participation in Privacy Shield). Doing so gives better protection to the rights of EU-based data subjects, by enabling them to send postal requests inside the Union (postal requests sent outside the EU increase the time taken to receive a response and the likelihood of a request being lost – or creating a more-effective defence for a recklessly non-compliant data controller / processor that the request was "lost in the post"). Accordingly, we believe that a physical EU address should be included in almost all privacy notices which purport to be compliant with GDPR.

When the issue of GDPR Representatives has been raised with the US Department of Commerce, which administers Privacy Shield in the US, their response has generally been to dismiss this requirement because it only applies to companies with no EU location – but while many Privacy Shield participants do have an EU establishment, around two thirds of those surveyed for this research had no location in the EU mentioned on their website, so it would appear necessary for them to have made this appointment to prevent them being in violation of GDPR.

We don't believe the failure to appoint an EU Representative lies wholly with the companies which should have done so; we suspect the majority of companies which are obliged to make this appointment would have, had they been aware of this 'hidden obligation'[3] – the difference between compliance with the privacy notice requirement (which must be provided as part of the self-certification process) and EU Representative obligations – 96.4% had a privacy notice easily available compared to 6.6% of companies with no EU establishment having appointed an EU Representative – is significant in reaching this conclusion.

1. *GDPR Articles 3 & 27, and Recital 80*
2. *GDPR Article 27(2)(a)*
3. *www.iapp.org/news/a/is-article-27-the-gdprs-hidden-obligation/*

Recommendations

Having considered the results of this research, we make the following recommendations:

Recommendations for companies transferring EU personal data from the EU to the US:

- Review the proposed data recipient's website for obvious issues
- Check Privacy Shield (or its replacement) to verify the recipient's participation
- Include a requirement in data processing agreements that an EU address or EU Representative contact information be provided

Recommendations for Privacy Shield's replacement:

- Strengthen the process by which independent verification of GDPR compliance is undertaken, perform brief reviews of self-certifying participants to verify their declarations, and undertake audits of a proportion of participants
- Participants should declare an EU establishment or the contact details of their EU Representative and include the EU-based address on the Privacy Shield website (in addition to a US address, if necessary)
- In line with GDPR, participants should be expected to respond to requests within one month, not 45 days

Recommendations for the EU data protection authorities:

- Clarify the types of additional safeguards which are anticipated to supplement SCCs where personal data transfers are made to the US (and other countries which have not been deemed adequate)
- When producing new SCC templates, include a requirement that the recipient provides the address of an EU establishment or contact details of their EU Representative
- When considering compliance as part of an investigation or complaint, start with a quick check to consider the most easily-assessed aspects of that company's GDPR approach: specifically whether they have a privacy policy, if they seek adequate consent for the use of cookies, if they have an EU establishment or Representative and/or have failed to appoint a data protection officer (DPO) where they work in a sector which would anticipate such appointment (e.g. medical). When taking a risk-based approach, those quickly-assessed factors can help inform the extent to which further investigation which may be appropriate
- If an EU-based postal address is expected to be made available to EU data subjects (unless the EU data processing is genuinely occasional), clarify this by way of guidance

Detailed results

The detailed results of the research are set out below, along with commentary on each aspect considered. The orange fields indicate an apparent failure to meet GDPR requirements.

Which Privacy Shield were participants enrolled in?	
EU-US Privacy Shield	**Swiss-US Privacy Shield**
384	286
100%	74.5%

The study considered whether companies were signing up to both Privacy Shield mechanisms, or only one. All companies surveyed had signed up to the US-EU Privacy Shield, and only around three quarters had signed up to the US-Swiss Privacy Shield.

The detail of the Privacy Shield notices (either separately or as part of the wider privacy notice) were not considered, but one notice was observed referring to being a participant in both mechanisms where they had only certified to one, and another referred to the Safe Harbour mechanism, which was replaced by Privacy Shield in 2016.

What verification method was used to confirm Privacy Shield compliance?			
Self-assessment	**TRUSTe**	**Other**	**Total**
356	23	5	384
92.7%	6.0%	1.3%	100%

As one of the pieces of information available on the Privacy Shield website, the verification method was considered as part of the survey. The vast majority achieved Privacy Shield certification following a self-assessment, with TRUSTe being the most popular verification method for those participants which had used an external method.

Is an EU contact address included on Privacy Shield website?		
Yes	**No**	**Total**
2	382	384
0.5%	99.5%	100%

An address is included on the Privacy Shield website for each participant under the heading "If you have a question or complaint regarding the covered data, please contact *[participant's company name]* at:".

On the presumption that (a) any company or individual wishing to enquire about Privacy Shield compliance would be EU-based or seeking to transfer EU data to the participant, and (b) that to be compliant with GDPR the participant would have an EU establishment or have appointed an EU Representative, it would appear to meet the Privacy Shield principles of 'Access' and 'Notice' more effectively if that address were EU-based.

Despite this, almost every participant lists a US-based address in this section. Even companies whose head office is in the EU (or UK) generally list a US-based address here, presumably as a result of the manner in which the information from participants has been transcribed to the Privacy Shield website.

It was also noted that "Privacy Shield organizations must respond within 45 days of receiving a complaint", despite the GDPR response period being one month.

Does participant have an EU establishment or an EU Representative (and is an EU address included on their privacy notice)?

Has an EU establishment		Has no EU establishment		Total
134		250		384
34.9%		65.1%		100%
Not applicable: no Representative required due to EU establishment		Appointed an EU Representative?		Total (where no EU establishment)
		Yes	No	
		19	231	250
		7.6%	92.4%	100%
Lists EU address on privacy notice	No EU address on privacy notice	Lists EU address on privacy notice	No EU address on privacy notice	Total
50	84	15	235	384
13.0%	21.9%	3.9%	61.2%	100%

Where a company is impacted by GDPR but has no EU establishment, GDPR Article 27 requires them to appoint a Representative in the EU, primarily to act as a point of contact to ensure EU data subjects have a route to access their right (and so that EU Data Protection Authorities have a route to raise questions and concerns) with the data controller or processor outside of the EU.

The degree of non-compliance with this obligation (over 90% of companies required to make this appointment had failed to do so) suggests that this GDPR obligation is simply not reaching the companies to which it applies. It is telling that the privacy notice requirement (which is a specific obligation under Privacy Shield) is met by over 96% of participants, but the appointment of a Representative (which is not mentioned during the Privacy Shield process) is met by fewer than 8% of those who require it.

Although not relevant until the end of the Brexit transition period (anticipated to be 31 December 2020 at the time of writing), it is worth noting that the largest number of EU establishments listed by Privacy Shield participants were in the UK. After the Brexit transition those UK locations will no longer be considered EU establishments, so an EU Representative may be needed by those participants at that time.

Use of cookies and whether consent process is GDPR compliant?				
Site doesn't use cookies	**Site uses cookies, no consent sought**	**Site uses cookies, consent sought in uncompliant manner**	**Site uses cookies, consent sought in purportedly compliant manner**	**Total**
12	154	148	70	384
3.1%	40.1%	38.6%	18.2%	100%

A cookie consent process was deemed compliant where a notice automatically appeared on the website at the first visit giving the visitor an option to refuse the use of unnecessary cookies, or provided a link to a page or pop-up which enabled that choice. Notifications that cookies are deemed accepted by the visitor's continued use of the site, pre-ticked consent boxes or messages indicating how to change browser settings to refuse cookies were deemed not compliant. A consent process which required cookies to be accepted to enable access to view the website would also have been deemed non-compliant, but this method was not seen across the sample group.

Over two thirds of Privacy Shield participants failed to meet the GDPR requirement that personal data (i.e. IP addresses or device identifiers) should only be processed by way of cookies where adequate consent has been obtained. A large number of participants use a cookie banner or similar, but without giving an option to opt out of the cookies or having the consent boxes pre-ticked by default, preventing the data subject making a clear positive action to indicate their consent.

For context, it is worth noting that this is not only an issue for US companies and/or Privacy Shield participants; many companies, including those in the EU, continue to operate cookies on their websites without having adequately obtained consent to do so.

For more detail on the investigation of cookies, particularly with respect to the application of the ePrivacy Directive to their use (which is outside the scope of this research), we recommend reading the Irish Data Protection Commissioner's report of 6 April 2020[4], which includes more detail on the issues of whether cookies are "necessary" to the operation of a site and the extent to which declining cookies via a consent portal resulted in those cookies not being used. Our research, although less-detailed, doesn't contradict any of the findings in the DPC report, and we support their recommendations.

4. https://dataprotection.ie/en/news-media/publications/report-dpc-use-cookies-and-other-tracking-technologies

Is a privacy notice available on the participant's website?				
Privacy notice one click from home screen	**Privacy notice two clicks from home screen**	**Privacy notice only available from Privacy Shield website link or cookie banner**	**No privacy notice or cookie policy only**	**Total**
348	21	7	7	384
90.9%	5.5%	1.8%	1.8%	100%

The vast majority of Privacy Shield participants have made privacy policies available on their website, usually via a link on the bottom of their website (although some links are easier to find than others, particularly when set out as black text on a black background, as was the case with one).

Where it was necessary to click twice to reach the appropriate policy, this was often due to the first click providing the data subject with options for a second click to take them to the most-relevant information – so that they didn't have to read through a bulky policy to find the part relevant to them – which is to be welcomed.

Did the link from the Privacy Shield website to the participant's privacy notice work?					
Yes	**Link to Privacy Shield policy**	**Link to a different privacy notice than available from website**	**Link to Privacy Shield website**	**No privacy notice and other***	**Total**
290	38	15	11	30	384
75.5%	9.9%	3.9%	2.9%	7.8%	100%

* - "other" includes links to terms of business / different company, website noted as 'unsafe' by virus checker.

For each Privacy Shield participant there is a link from the Privacy Shield website to the privacy notice. For the most part these links worked, but some directed to a separate Privacy Shield notice, some links didn't work, and some simply directed back to the Privacy Shield website.

It would appear to be a simple step for the administrators of the Privacy Shield to establish whether these links operate as expected at commencement (and when updated).

Methodology

Hypothesis: Participants in the EU-US Privacy Shield are compliant with GDPR.

Aim: To establish whether the hypothesis is inaccurate, using information publicly available on Privacy Shield participants' websites (noting that it will not be possible to establish overall compliance from this information, but it will be possible to identify areas of likely non-compliance)

Scope of Study:

- Selection of sample group:
  - Sample size of 384 chosen, being the number for a population size of over 5,000 (5,248 participants listed on website at 12 September 2020) which would return an error factor of +/-5%[5]
  - Sample participants randomly chosen by using the random number generator in Microsoft Excel to produce 384 numbers between 1 and 5,284 (adding 1 to duplicate numbers), and allocating those numbers to participants in alphabetical order as set out in the Privacy Shield website
- Online review is based on observations of websites from a UK-based IP address between 12th September 2020 and 1st October 2020
- Research was undertaken on the site which appeared in the UK when searching using the domains listed in the Privacy Shield website from the link in the "Privacy Policy" section (the domain for the email contact was used as a second option for the site if there was no privacy notice link – not primary because that email may be for an external DPO)
- Only considering main website, not subsidiaries, other covered entities or apps
- Where there are several privacy policies listed on the Privacy Shield website (e.g. due to several group entities being covered by a single Privacy Shield participation), the most relevant one (same name as primary participant) was inspected
- Companies which declare a subsidiary as Representative are noted as having an EU establishment and not a Representative, although either could be argued

5. *http://www.tools4dev.org/resources/how-to-choose-a-sample-size/, http://www.beaumontethics.ie/docs/application/samplesizecalculation.pdf*

The following outlines the process followed during research for each website reviewed:

1. **Relevant page on the Privacy Shield website opened for each participant in sample group (using Google Chrome browser)**

2. **Privacy Shield website page checked for:**

   a. Is the participant participating in EU-US and/or Swiss-US Privacy Shield?

   b. What method did they use to verify the requirements of participation?

   c. Was an EU/UK located address included in the "Questions or Complaints?" section?

   d. What is the web address of their website (using the privacy policy link – where included – as the primary source, and the email contact as a secondary)?

3. **Participant website opened on different browser (Microsoft Edge) and checked for:**

   a. Cookie consent – does the site purport to adequately seek consent for the use of cookies?

   A cookie consent process was deemed compliant where a notice automatically appeared on the website at the first visit giving the visitor an option to refuse the use of unnecessary cookies, or provided a link to a page or pop-up which enabled that choice. Notifications that cookies are deemed accepted by continued use of the site, pre-ticked consent boxes or messages indicating how to change browser settings to refuse cookies were deemed not compliant.
   A consent process which required cookies to be accepted to view the website would also have been deemed non-compliant, but this method was not seen across the sample group.

   b. Privacy notice –

   i. Is one available?

   ii. How many clicks from the front page did it take to reach it? (Note: this is clicks from home-screen – if a re-direction screen shown first, that isn't counted)

   iii. Did it refer to participation in Privacy Shield?

   iv. Is a physical address in the EU included?

   v. Has an EU Representative been appointed?

4. **Returning to Privacy Shield website page on first browser, opening the link in the "Privacy Policy" section:**

   a. Did the link open the participant's current privacy notice?

   b. Are cookies being used ('EditThisCookie' browser extension[6] used to assess) (where no cookies on "Privacy Policy" page, home page also checked)?

6. *www.editthiscookie.com/*

DataRep

DataRep is a leading provider of the EU Representative service under Article 27 of GDPR, with a unique network of 28 contact locations across the EU and UK. DataRep is a member of the International Association of Privacy Professionals (www.iapp.com), and a supporter of the Pledge 1% charitable initiative (www.pledge1percent.org). For any enquiries about this research, our GDPR EU Representative service, or the UK Representative service which will be required after the Brexit transition, please feel free to contact us at contact@datarep.com.

DataRep would like to thank Ralph O'Brien of REINBO Consulting (www.reinboconsulting.com) for his assistance and input to this research.