create with context

iapp

The UX Guide to Getting Consent

THE UX GUIDE TO GETTING CONSENT

In the EU's General Data Protection Regulation, set to come into force in May of 2018, the word "consent" appears 72 different times. In truth, consent is at the very heart of data protection and privacy — the data subject must have a say in how personally identifiable information is collected, used, shared, and destroyed.

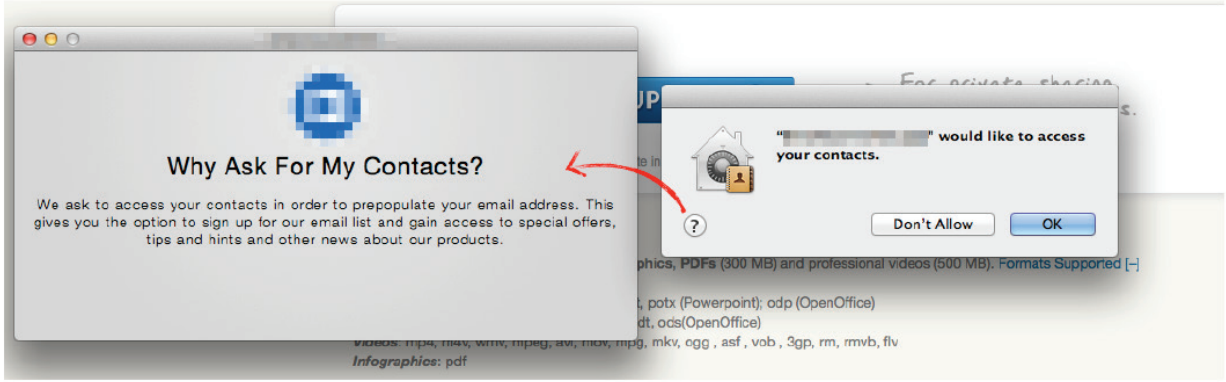
However, one word is conspicuously absent from the GDPR: "notice." Actually, it appears a single time in the document, but in a setting that's irrelevant to data subjects. The GDPR says that the EU Commission must give notice to a third country when revoking an adequacy decision for trans-border data flow, but doesn't say anything about how organizations should give notice to data subjects about how their data is being collected, used, shared, and destroyed.

Thus, organizations are left to fend for themselves as they go about acquiring consent. While they also need to create a way to track what consent is attached to what data, figure out how to allow data subjects to revoke consent, and many other technical issues, first and foremost is the user experience. The UX. The user interface.

At some point, the data subject is going to be presented with some sort of interface and be asked to provide, with some "unambiguous indication," consent for whatever processing is being requested or required. This interface might be a piece of paper where the data subject signs at the bottom. It might be a question spoken aloud by a smart device where the data subject verbally assents. It could be anything from the push of a button to the toggle of a radio button to the tick of a box (but we'll get to that later).

Further, there are nearly infinite variations in the ways all of these controls can be presented, via colors, images, animations, vocabulary, languages, and the like. All of these design decisions are part and parcel of acquiring consent in a way that is not only legal, but also effective.

YOU HAVE TO CLICK ON THE '?' TO FIND OUT HOW YOUR CONTACT INFORMATION IS USED



Is consent "informed" if the user has to click another button to understand what they are agreeing to?

CONTINUED

How do you choose what to provide so as to ensure you are complying with the GDPR and using, for example, "clear and plain language," in an "intelligible form"? At the same time, how do you make sure being legally compliant doesn't create barriers to acceptance caused not by "creeping out the user," but simply because the process is tedious, ugly, or unwieldy?

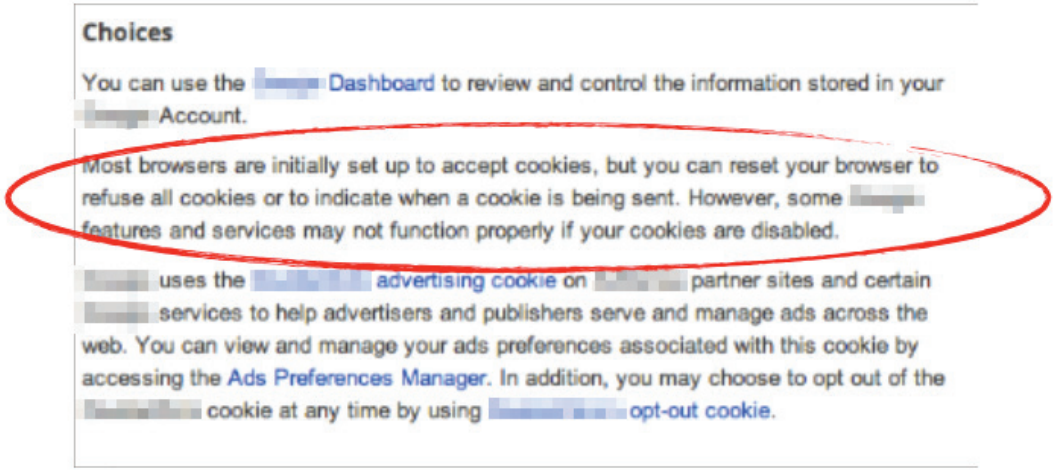
Such are the questions that Ilana Westerman and her Create With Context team have researched and continue to explore as they create benchmarks, best practices, and effective mechanisms in the digital arena. In this collaboration, the IAPP has identified and expanded upon the many ways the GDPR requires consent, while Create With Context paired those consent requirements with research-based UX examples of how to meet the GDPR's needs.

It's important stuff. We assume you don't need to be reminded of the GDPR's significant fine structure: up to 2 and 4 percent of global turnover, depending on the nature of the infraction. If consent is involved, the infraction will almost always trigger the latter.

TO CONSUMERS, THIS IS VAGUE, NOT SPECIFIC

"if you turn off cookies... some features and services may not function properly." What does that mean? What will be the impact?

Is consent "specific" if the user has to guess what features might not work if they don't consent?



DEFINING CONSENT

In Article 4, the GDPR lays out clearly what is meant by "consent" in the first place. It is something that signifies agreement to the processing of personal data that is:

FREELY GIVEN: To define this, it's easier to discern what is not "freely given" rather than what actually is "freely given." For instance, in the context of an employment situation, the Article 29 Working Party has made clear that "consent is highly unlikely to be a legal basis for data processing at work, unless employee can refuse without adverse consequences."

This is directly related to Recital 42, where the GDPR reads, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

Further, in Article 7, the GDPR explains that, "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

In other words, if your app doesn't need location data to work, you can't ask for it as a condition of using the app. Nor can you bury a slew of unnecessary conditions in terms and conditions that must be agreed to before using a service.

SPECIFIC: Per Article 6, this means that the consent you are requesting must be for "one or more specific purposes." Blanket consent for future processing is simply not allowed. It must be clear why you are requesting personal data and what you plan to do with it.

INFORMED: One cannot assume that data subjects understand the law and their rights. At the point of collection of consent, as outlined in Article 13, the data subject must be informed that they have the right to withdraw consent "at any time."

Further, if you are, for example, collecting data through a registration page and some of the data being provided is not particularly necessary for the performance of the service or contract, it should be clear which data falls into the "required" category and which does not.

It's also important to avoid legalese as a defense mechanism. The information provided should, says Recital 42, "be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms." It's fair to wonder what "clear and plain language" means in the European Union, where an organization may be collecting consent from data subjects speaking any number of languages.

Finally, to be considered "informed," says Recital 42, "the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended."

Specifically, at the point of collection, the data subject must be notified of:

- Who the controller is, with contact details, along with the details of any third-party representative.
- The contact details of the data protection officer.
- Why the data is being processed and why it's legal to do so.
- The categories of data to be collected.
- If you're going to transfer the data outside of the EU and why it's legal to do so.

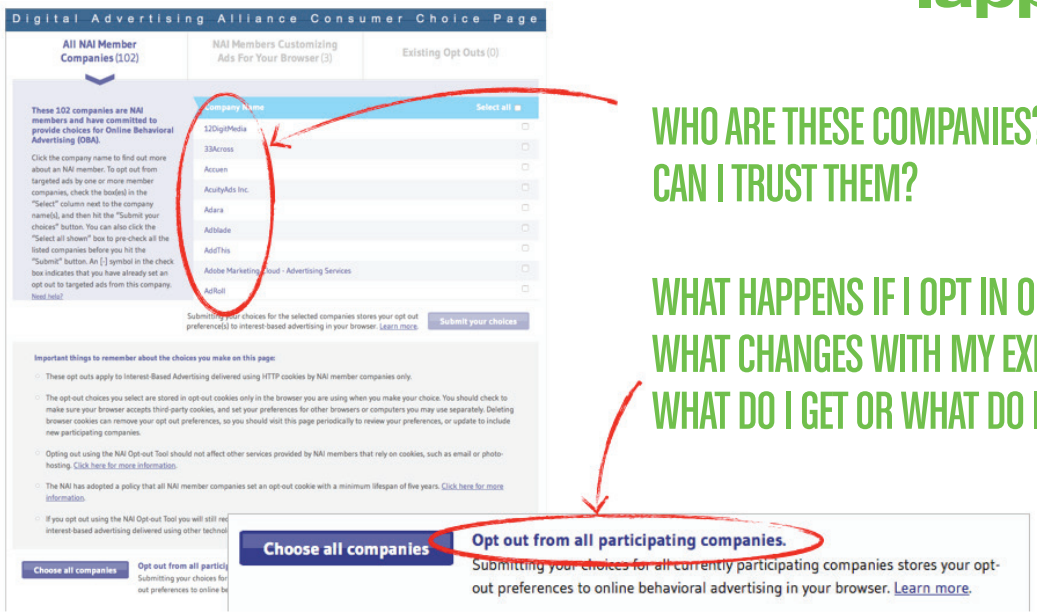
DEFINING CONSENT CONTINUED

UNAMBIGUOUSLY INDICATED: The word "unambiguous" appears both in Article 4 as part of the definitions, and in Recital 32, but nowhere is an example of "unambiguous" provided, other than with examples that are in combination with "clear affirmative act" (see below). It's safe to assume, then, that we should take this at face value. It should be obvious to data subjects what they are consenting to.

A STATEMENT OR CLEAR AFFIRMATIVE ACTION: Recital 32 is clear on this front: "Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

The same recital also says that "choosing technical settings for information society services" does, indeed, fall under the definition of an "affirmative act." So, when combined with "privacy by default," gathering consent for a broad swath of data collection might be as simple as pointing users to a settings panel in the set-up process and allowing them to toggle radio buttons for those categories of data with which they're comfortable providing consent. Research shows, however, that this is not a particularly good way for gathering informed consent and tends to drive opt-outs.

However, things like written statements and oral statements are the safest and most obvious ways to accomplish this.



WHO ARE THESE COMPANIES?
CAN I TRUST THEM?

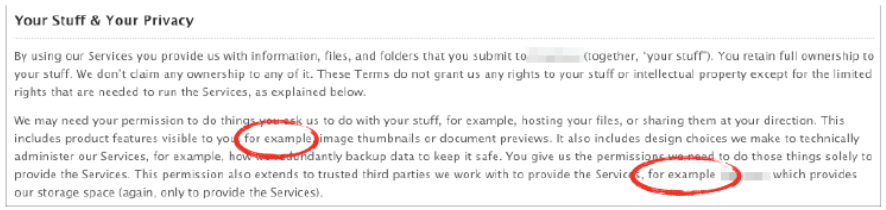
WHAT HAPPENS IF I OPT IN OR OUT?
WHAT CHANGES WITH MY EXPERIENCE-
WHAT DO I GET OR WHAT DO I LOSE?

Combining "specific" and "informed" can be tricky. Don't sacrifice one in the name of the other.

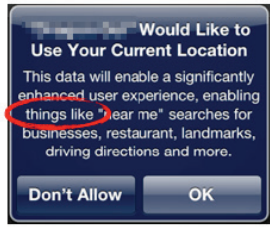
IT MIGHT BE CLEAR PLAIN LANGUAGE, BUT HOW DO THEY INTERPRET IT? IS IT REALLY CLEAR?

For many users, terms like "such as", "things like" and "for example" all means "equals". They don't see the bigger pricture of what else they could be agreeing to.

"For example" is read as "equals".



"Things like" does not fully convey all the possibilities.



Is consent "unambiguous" if the very terms you use to collect it are ambiguous?

EXPLICIT CONSENT

In certain cases, the General Data Protection Regulation calls for a special type of consent: "Explicit consent." You might be forgiven for thinking "unambiguous" and "explicit" are synonymous, but the framers of the GDPR made a point to distinguish between the two. It is not a coincidence that they consistently use each of these terms in specific settings throughout the document.

Both, to be sure, require an "affirmative action" and a "statement or conduct" that clearly indicates the data subject understands what they are consenting to. However, remember that "choosing technical settings for information society services" is an affirmative action. It may be that a setting in an app is appropriate for providing "unambiguous" consent, but would not be considered providing "explicit" consent, as it would be painting with too broad a brush.

"Explicit" consent should be seen as direct action and correlation, either a direct statement along the lines of "I consent to …," or the checking of a box or clicking of a button next to words that say things like, "By checking this box, you consent to …" While this is legal, however, research shows data subjects often consent without actually knowing what they're consenting to.

In cases where only unambiguous consent is required, it may be that certain forms of implied consent are acceptable. If a data subject is using a mapping app created by a certain company to navigate a city, and has previously allowed for location tracking in global settings tied to the user account for that company, and sees their dot moving through the map as they travel, that is almost certainly unambiguous consent, but is not explicit consent, for example.

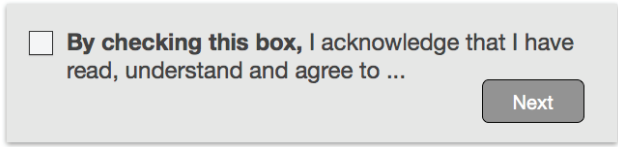
The GDPR outlines three main areas where explicit consent is required:

SPECIAL CATEGORIES OF PERSONAL DATA: The GDPR, in Article 9, carves out a certain subset of personal data that is particularly sensitive and thus is treated differently under the law: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, for example, or health and biometric data. Also, data that might concern a person's sexual orientation or sexual habits is sensitive.

However, do not consider that list finite and complete. As Recital 51 makes clear, this sensitive data is data that, by its nature, is "particularly sensitive in relation to fundamental rights and freedoms." If the data might in some way infringe on a data subject's dignity, equality, or ability to find solidarity and justice, you should consider that data

EVEN IF IT IS SPECIFIC, IF THEY DON'T READ IT THEY ARE NOT INFORMED

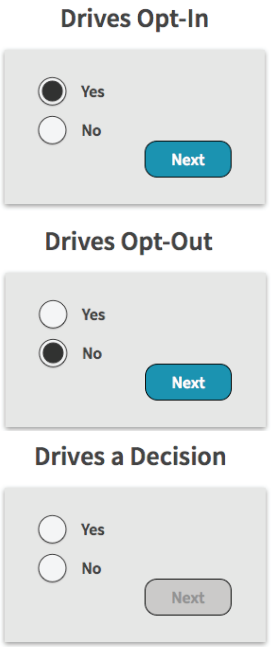
FEELS LIKE A REQUIREMENT, NOT A CHOICE… People have become conditioned to having to agree to T&Cs. They have tuned it out. They automatically tick the box, but don't read what they are agreeing to.



ACTIVE OPT-INS DRIVE A PERSONAL DECISION

NOT COMPLIANT - NOT ACTIVE CHOICE

COMPLIANT people are more likely to become aware when they have to make a decision



Just as a "pre-ticked box" is not unambiguous consent, neither are pre-set controls. The user should make an active decision.

EXPLICIT CONSENT CONTINUED

sensitive and take care to only process it either via explicit consent obtained from the data subject, or via one of the other derogations, such as to comply with EU member state law or in the public interest.

AUTOMATED DECISION-MAKING: Article 22 of the GDPR says that a data subject should not be subject to a decision made solely via automated processing that produces "legal effects" or "significantly affects" them, unless that processing is based on explicit consent, or other standard derogations like fulfilling a contract.

Some relatively obvious cases where automated processing is likely to be allowed by member state law are carved out in Recital 71, such as the case of tax-evasion monitoring and prevention in a financial services setting. If you're using automation to ensure security and reliability of a service, that's also expressly allowed.

However, even with explicit consent, there are specific notice requirements indicated in Recital 71 as well. For example, there should be "specific information to the data subject" on their right to human intervention, "to express his or her point of view," and to receive an explanation of any decision made and be able to challenge that decision. Further, children should almost never be subjected to automated decision-making, as they cannot understand those specific explanations.

TRANS-BORDER DATA FLOW: While there are any number of appropriate methods for transferring personal data outside the borders of the EU — from country adequacy to model contract clauses to binding corporate rules — Article 49 does allow for explicit consent as a valid basis for moving personal data. It is literally a "derogation for specific situations."

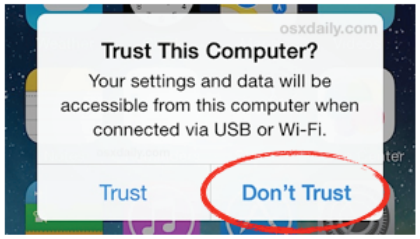
As part of gathering the explicit consent in this case, the data subject must be informed of the possible risks that data transfer might present to their rights and freedoms. In addition, the GDPR makes clear this should not be a regular occurrence. This carve-out for trans-border data flow should be used in "certain circumstances" and "where the transfer is occasional," according to Recital 111.

PEOPLE ARE AS LIKELY TO BE INFLUENCED BY A 'PROMOTED CHOICE' AS THEY ARE BY A DEFAULT OPTION

NOT COMPLIANT -
NOT ACTIVE CHOICE

PROMOTED CHOICE IS EFFECTIVELY A DEFAULT. SO IS IT COMPLIANT?

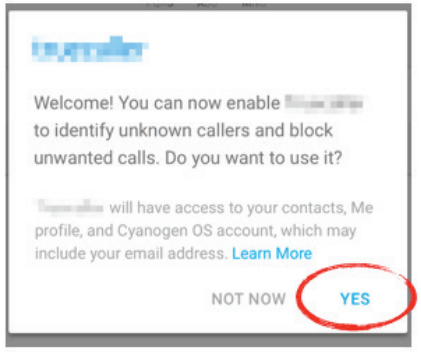
Promoted Choice



"This is what the majority would select; am i an outsider?"

"The company is the expert, this must be what is the best."

Heavily Promoted Choice



Is the user making an active decision if the decision seems pre-ordained?

CHILDREN

The General Data Protection Regulation, for the first time in an EU-wide privacy legislation, makes specific allowances for children (classified as "vulnerable natural persons") and sets an age of consent: 16. If the child is below the age of 16, processing of that child's personal information is not allowed unless consent is provided "by the holder of parental responsibility over the child."

However, this is an area where you'll have to pay close attention to individual member state laws. While the GDPR is meant to standardize data protection law across the EU, in this case member states may set a lower age of consent, but not lower than 13 years of age.

Thus, you may have to have different notice and consent mechanisms for children for each member state, depending on how all of them implement this piece of the GDPR. Only if the data is being processed in the context of offering counseling services to the child is the parental consent not necessary.

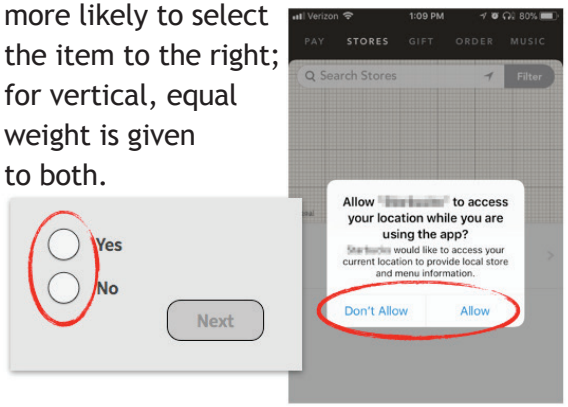
Special attention for children is also discussed when the GDPR sets transparency requirements. The notice provided, if in a setting where children are likely to be among the readers, "should be in such a clear and plain language that the child can easily understand." Further,

CHILDREN

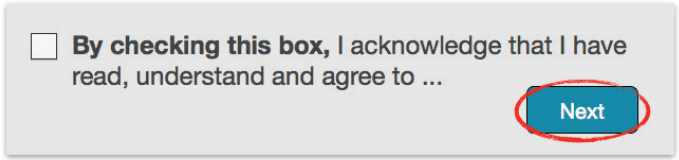
EVEN IF A CHOICE DOESN'T APPEAR TO BE PROMOTED, WORDING, WIDGET AND SEQUENCE MATTER

HORIZONTAL VS. VERTICAL CHOICE

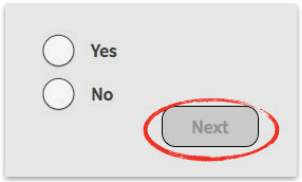
For horizontal, much more likely to select the item to the right; for vertical, equal weight is given to both.



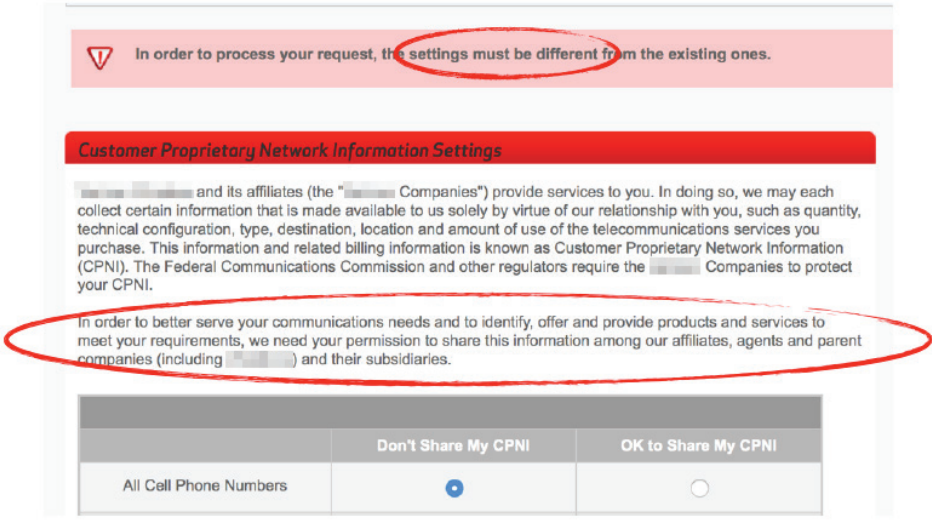
People are much more likely to quickly proceed without reading or processing information if button is enabled.



Grayed out buttons are not active, and signal thatyou have to pause and decide to proceed.



If you want to emphasize trust, emphasize that there is a choice.



I HAVE TO DO IT. WHAT IS MY OPTION? BUY A NEW PHONE, NEW CAR, ETC. WHO IS TO SAY THEY WILL NOT CHANGE THEIR POLICIES TOO?

Why give a choice when there is no choice?

Maybe consent is not the right compliance tool at all. Should you instead be relying on legitimate interest or other derogations?

CHILDREN CONTINUED

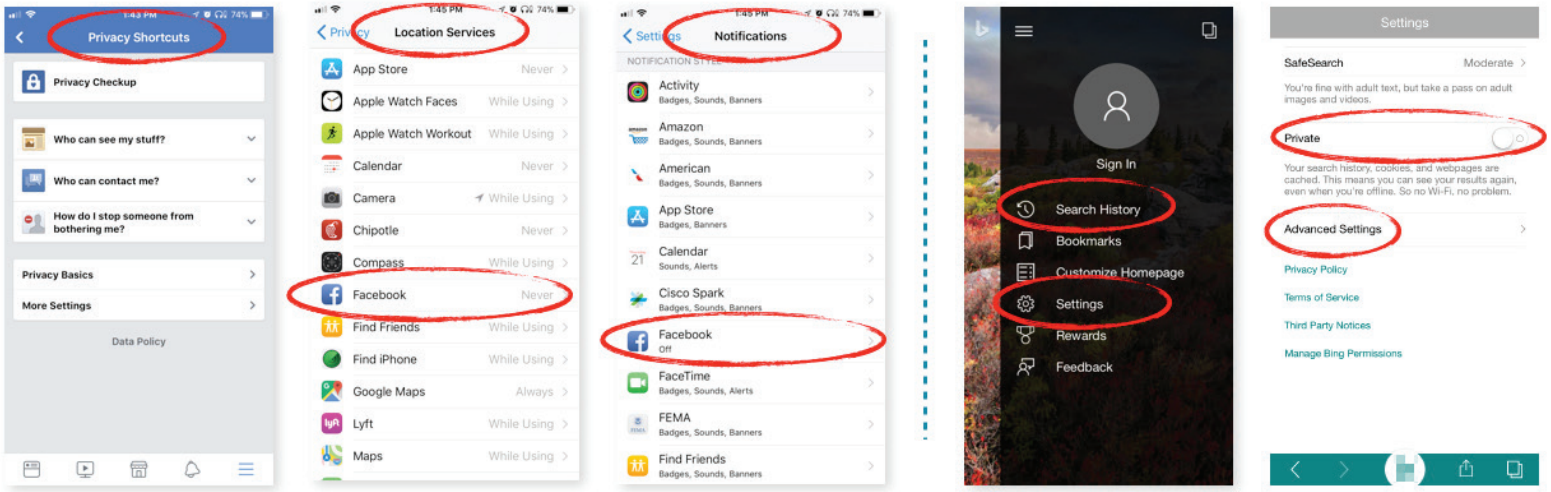
when setting up right to be forgotten procedures, remember that the right is "particularly relevant" if consent was given when the data subject was a child, so it will be important to distinguish in filing systems whether the data subject was a child when consent was provided.

But how do you determine whether the consent being provided is actually being provided by the authorized holder of parental responsibility? It can be tricky. The GDPR requires that the controller "make reasonable efforts" to verify the consent is being provided by someone with parental responsibility, "taking into consideration available technology."

What does that mean? EU data protection authorities may look here to efforts that have been undertaken in the United States as part of compliance efforts for COPPA (the Children's Online Privacy Protection Act). The Federal Trade Commission has established a series of "acceptable methods" under COPPA for obtaining a parent's "verifiable consent." These include:

- A signed consent form sent via fax, mail or electronic scan.
- The use of a debit card or credit card.
- Calling a toll-free number staffed by trained personnel.
- Provision of a government-issued ID you can check against a database (but make sure you delete it afterward, so you don't collect yet more personal information).
- Provision of a government-issued ID you can check against a second photo provided, using facial recognition technology (this may not be practical in the EU, given the carve-out for biometric data).
- Answering a series of questions that only an adult could be deemed to know.

Without guidance from data protection authorities, organizations will have to use their best risk-based judgment when determining whether "reasonable" efforts have been taken to verify that the parent is, indeed, the parent. Many web sites choose to include terms and conditions that disallow children and actively try to avoid collecting children's data.



DISPERSED CONTROLS CAN BE HARD TO FIND

Multiple locations for settings, not consolidated.

User settings can be an effective way to get unambiguous consent, but if they are dispersed, can the user find them all?

PRIVACY BY DESIGN: INSERTING ONESELF IN THE DESIGN PROCESS

While "privacy by design" gets a lot of attention, Article 25 of the General Data Protection Regulation is among the document's shortest. What does privacy by design look like? It's hard to know. The GDPR merely says that organizations must "implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing."

That's it.

It's therefore important to understand the design process in order to understand where "organizational measures" might be applied. Where should privacy and data protection professionals be involved? It is certainly well understood in many organizations that privacy and data protection are often brought to the table much too late, often after the product or service to be released has already been designed, constructed, tested, and readied for release.

This can lead to massive inefficiency and, frankly, bad feelings toward the privacy office. Privacy and data protection are much more than simply the "legal review" stage.

Further, it's also the case that privacy professionals will often implement consent-gathering solutions without consulting designers, leading to inelegant, and ineffective, mechanisms that fail merely for their clumsiness.

Essentially, there are four main points in every product or service launch where privacy and data protection should be involved and consulted.

1. The idea stage: Some people might refer to this as the "white board" stage, or product inception. Regardless, it's the beginning of the project where people are defining the business case or why it helps a public body serve its constituency.

This is "design" at its grandest scale, the literal design of the idea. If this "Big D Design" is based upon personal data processing that's unlikely to be legal under the GDPR, it is doomed to fail. Better to find that out early than late, after organizational resources have been expended.

2. The requirements stage: Here is where the fine details begin to be worked out. Perhaps this is where marketing gets involved and talks about targeting the right population and who might be interested in the product. Maybe choices need to be made at this point about which populations will be targeted.

The privacy and data protection professional will need to be involved here to help understand what limitations might exist, what opportunities can be taken advantage of, and how the design of the product might limit effectiveness or enhance it based on how personal data might be collected and used.

3. The design and development stage: This is where the coding happens. How will the data travel? Who will see it along the way? What third parties will be involved? Clearly, privacy is vital to efficiency here. Moving from stage two to stage three, the data protection team should be able to offer suggestions and advice before the coding happens so that rework is limited.

Further, this move from "Big D" to "little d" design is where the work that most people think of as "design" happens. It's the look and feel of the product or service, how people will engage with it, what's often known as "user experience," "user interface," or simply UX or UI.

Is there going to be animation? A video? Lots of text or lots of pictures? When and where will users be asked for consent and how will it be done? When done well, users won't even notice the design choices you make. When done poorly, users will abandon, complain, and get frustrated with the product or service in a way that is going to make gaining appropriate consent unlikely.

4. The test and deploy stage: Finally, it's time to put the product or service out into the world and see how it performs. The privacy and data protection team will want to stay involved through this stage in order to see how consent mechanism are performing, along with making sure data minimization and transfer efforts, among other things, are operating as engineered.

Is the data traveling someplace unexpected? Are new vendors being used in ways that weren't predicted from the outset? Has any guidance, law, or interpretation changed in the interim between design and delivery?

For some products and services, this stage may continue indefinitely, as the new iterations are released and feedback is incorporated. In the world of privacy by design, a privacy professional's job is truly never done.

publications@iapp.org
iapp.org

info@cwcmail.com
+1 408 834-7601
createwithcontext.com