• Privacy in the product design lifecycle

Ico uk 14/03/2023 https://ico.org.uk/for-organisations/privacy-in-the-product-design-lifecycle/

Indice generale

• Legals

Unofficial pagination

This text is unofficial, you can find the latest versione on Ico.co.uk.

Share it freely, unless the “unofficial” statement is highlighted.

https://ico.org.uk/for-organisations/privacy-in-the-product-design-lifecycle/

IusOnDemand srl (Italy) is specialized in legaldesign.it since 2014.

Proudly degoogled.

Follow us:

privacykit.it/newsletter newsletter (it, eng)

privacykit.it/podcast podcast (it)

Telegram:

privacykit.it/telegram - news aggregator from DPAs and Cert (eng, it)

Follow us on:

www.gdprkit.it - compare multilanguage GDPR (eng. it. eu)

privacykit.it - main web site (it, eng)

wpkit.it - specified for WordPress (it)

italian; english coming soon.

• Summary

If you’re making a product or service that involves processing personal information, it is important to consider data protection law throughout the design and development process. This includes kick-off, research, design, development, launch, and post-launch phases.

The case for privacy – Your organisation must comply with relevant laws. But there are also pressing reasons beyond legal compliance to prioritise privacy. For example, the risk of harming people and society itself, as well as the business risks to organisations.

Privacy in the kick-off stage – including kick-starting collaboration, mapping your product’s personal information needs, and ideas on weaving privacy into your business case.

Privacy in the research stage – including gathering up-front perspectives on privacy, testing of work in progress, and ways to protect the personal information of research participants.

Privacy in the design stage – including choosing the right moments, obtaining valid consent, and communicating privacy information in ways people understand.

Privacy in the development stage – including defining the appropriate amount of personal information required, exploring technical solutions that enhance privacy, and protecting personal information in development environments.

Privacy in the launch phase – including conducting pre-release checks, factoring privacy into rollout plans, and deciding how best to communicate changes.

Privacy in the post-launch phase – including monitoring and triaging fixes, reappraising expectations and norms, and celebrating privacy successes.

Further reading

- Data protection by design and default

1. About this guidance

This guidance is written for technology professionals such as product and UX designers, software engineers, QA testers, and product managers. It assumes your organisation acts as a data controller. Companies whose software, products, apps, or websites collect, manage, or share people’s personal information are likely to meet this definition. If your organisation acts as data controller, the organisation is responsible for complying with data protection law. Data protection obligations vary

for organisations that fall outside this category, such as those that act as processors for personal information.

This guidance will help you, as technology professionals, understand how to incorporate data protection by default and design in your development of a technology product or service. It is not a substitute for detailed ICO guidance, but is intended to help you understand how to navigate and apply our more detailed guidance throughout the product design lifecycle.

To help you to understand the law and good practice as clearly as possible, this guidance says what organisations must, should, and could do to comply.

2. Legislative requirements

Must refers to legislative requirements.

3. Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

This approach only applies where indicated in our guidance. We will update other guidance in due course.

Further reading

- What is personal data?
- Controllers and processors

• The case for privacy

Share(Opens Share panel)

We are responsible for regulating the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), and the Privacy and Electronic Communications Regulations (PECR). Throughout this guidance, you should take references to privacy law as referring to these three laws.

Your organisation **must** comply with these laws. But there are also pressing reasons beyond legal compliance to prioritise privacy. Privacy also has real-world impacts on people's rights and freedoms. Privacy-minded design will also benefit your organisation, reducing risks, saving time and expense, and ultimately helping you build better digital products.

4. Legal requirements

Under the UK GDPR and DPA 2018, your organisation **must** consider data protection and privacy issues upfront in everything it does. You **must** bake in privacy considerations from the design stage throughout the product development lifecycle. We may ask you to demonstrate how you have done this, if appropriate.
UK GPDR sets out seven key principles:

- lawfulness, fairness, transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

These principles lie at the heart of UK GDPR, informing everything that follows, and are key to your compliance with the regulation's detailed provisions. The principles should therefore underpin your design approach.

UK GDPR also gives everyone rights over how their personal information is used. These individual rights include a right to:

- be informed;
- access and receive a copy of their personal data;
- have inaccurate data rectified;
- not be subject to automated decision-making and profiling; and
- have personal data erased.

Organisations which act as controllers **must** ensure people can exercise these rights. Thoughtful design helps people have a good experience while doing this.

PECR sits alongside UK GPDR. If you send electronic marketing or use cookies or similar technologies, you **must** comply with this, alongside the UK GDPR.

Further reading

- Data minimisation
- Individual rights
- Direct marketing guidance

5. Privacy harms to people

Penalties and fines for violating data protection law can be severe. However, privacy is not just about legal compliance; failing to protect privacy can also have a significant impact on people. Overlooking privacy in the design process can lead to real harm and distress.

Information leaks can cause people stress and anxiety, as people worry about who might end up with access to their personal information. If data does end up in the wrong hands, it may lead to intrusions such as nuisance calls or, in some cases, even more serious harms such as extortion or fraud.

Vulnerable people can be particularly at risk. For example, people facing domestic abuse can be particularly endangered if their privacy is compromised. Evidence shows abusers commonly misuse sensitive personal information to harass and control their partners.

6. Privacy harms to society

Privacy issues also have social dimensions. For example, if people's votes were not secure and private, or if sensitive information such as political affiliation became public knowledge, there could be a serious impact on democracy and 'chilling effects' on freedom of belief. Violations of this sort can also exacerbate discrimination, furthering inequality against marginalised people. Privacy issues could also damage the role of law and justice if, for example, victims or witnesses felt unable to report crimes safely. A society that overlooks privacy is likely to be a less just society.

As designers become increasingly aware of their duties to society, not just people, it is important to consider the wider social impacts that could arise from your design decision-making.

Further reading

- Overview of data protection harms and the ICO's taxonomy

7. Business impacts

There are also important business reasons to prioritise privacy within the design process.

People are increasingly keen to choose providers that match their privacy expectations. Investing in privacy can help your product or service stand out and can build customer trust that leads to loyalty and positive word of mouth. Competitors hit by privacy problems, however, may suffer reputational harm, creating customer churn and brand damage.

Talented technologists are also becoming more selective about the companies they work with. Attention to privacy shows you foster a culture of doing things right, and of protecting people rather than cutting corners. Strong candidates motivated by positive impact are often drawn to these cultures, meaning a stronger candidate pool and enhancing your company's future competitiveness.

As you work through this design guidance, encourage your organisation to see privacy and data protection as investments, not costs. Privacy is a core product and UX issue. Organisations that embrace this have an opportunity to outshine their competitors by showing they truly care.

• Kick-off

Share(Opens Share panel)

You **must** consider privacy from the earliest design stage when planning new features or products. Start too late and you may have to make fixes later on that can prove expensive and delay your project.

8. Plan ongoing collaboration

You **should** involve other stakeholders in privacy discussions as soon as you can:

- You **should** identify your colleagues in data protection or legal teams if you have them. Introduce yourself and the project early. It's easier to discuss and resolve privacy questions as you go than at the end, when you may need to change key design decisions.
- Your organisation **must** have a lawful reason for processing personal information, and may need to complete a data protection impact assessment (DPIA) for your project. Discuss with your legal or data protection colleagues whether you could help with this work. A product or service might use different lawful reasons for particular features.
- You **should** also consult with other senior stakeholders, as required. For example, you may need sign-off from product leaders or technology teams. Plan milestones or activities to raise privacy issues with these stakeholders: don't just wait until final approval.
- You **could** record discussions and actions in a central location, such as an intranet or wiki. This will help teams who work on the product in future to see your working, and help you demonstrate compliance.

9. Map what personal information the product needs

Every product is different, and within a product different features often have quite different purposes:

- You **must** consider what personal information your product might use across its entire range of features. The definition of personal information is wider than many people realise, so check carefully.

- To keep track of the personal information you handle, you **could** create a visual map showing how you will collect and process information through your product. Keep this updated as the feature or product evolves.
- If any of the personal information you are processing is classed as special category data, your organisation **must** meet additional conditions to process it. This covers particularly sensitive personal information types such as religion, race, and sexual orientation, amongst others.
- If children are likely to access your service, even if they are not your target audience or user, you **must** consider the Children's code.
- You **should** consider how people will interact with your product. Is your interface graphical, textual (eg a chatbot), audio (eg a smart speaker), or something else? Every mode of interaction can raise different privacy concerns.

Example

A smart TV app asks people to log in. Since an on-screen keyboard could make password entry visible to others in the room, the designers as a matter of good practice offer an alternative. People can also log in through their smartphone and link the TV app directly.

Further reading

- What is personal data?
- Children's code design guidance

10. Identify changes and risks

Based on the data sources and flows you've identified, look for potential privacy risks that might arise:

- Your organisation **should** review whether new uses of personal information introduce new risks to people's rights and freedoms. In addition to information that people provide directly, your organisation **should** consider personal information you obtained by observing user activities, or that you infer or derive another way.

Example

A social media company wants to identify people who may have diabetes, by analysing whether they use certain keywords or read articles about the topic. Since health information is deemed special category data under UK GDPR, the company needs to meet additional conditions to perform this analysis.

- You **should** examine the relationship between your organisation and your user. If you hold a lot of information about people, or have significant power over them, privacy risks might be

higher. People may feel unwilling to exercise their rights or to give consent freely if they think it could disadvantage them.

- You **should** check whether your new product or feature could create knock-on privacy problems for existing features. For example, allowing people to edit private messages after they have been sent could allow hostile users to cover their tracks after leaking data.
- You **should** think about how bad actors or attackers could use new sources of data maliciously.

11. Agree responsibilities

Add time in your roadmap for privacy reviews and potential changes, and for validating your approaches through testing:

- You **should** agree with your stakeholders who is responsible for taking privacy decisions. If you have one, a data protection officer may have final accountability, but you should also consult senior stakeholders. Also, you **should** discuss who you need to keep informed about key decisions.
- You **should** talk with your engineers or developers about setting up appropriate logs or alerts. You **could**, for example, build systems that alert teammates to privacy-threatening bugs, or to capture audit trails of what happens with personal information and who accesses it in the system.

12. Weave privacy into your business case

Early in a project's life you will have to explain the value of the work. This is a perfect opportunity to discuss the advantages privacy offers and how you might measure them. For example, you **could** do the following:

- Communicate the value of privacy in your business case. This could include reducing the risk of damaging mistakes, or lowering likely support costs by allowing people to exercise their individual rights directly.

- Embed privacy into your success metrics, so you meet desired outcomes while still keeping people's personal information safe. Privacy-specific KPIs or OKRs (objectives and key results) can also help you monitor privacy issues and provide early warning of problems.
- Discuss how privacy-enhancing methods lend you an advantage over competitors. If people feel safe on your platform, this may lead to more loyal use and a trustworthy reputation that can differentiate your sales and marketing.
- Write a pre-mortem – an imaginary article looking back from the future on your feature's perfect launch or failure – to help you focus on the privacy aspects that will ensure success.

• Research

Share(Opens Share panel)

Research covers user research, UX research, or design research that technology teams run to understand user needs and evaluate product choices. The UK GDPR and DPA 2018 contain research provisions that refer to personal information processing carried out for a) archiving purposes in the public interest, b) scientific or historical research purposes, or c) statistical purposes. Most user research is not covered by these provisions. Therefore, in this guidance, ‘research’ refers to user research, not the research provisions covered in privacy law.

User research helps you learn about people’s privacy needs and concerns so you can create products that people trust.

13. Survey the landscape

Just like the world of technology, the world of privacy is constantly evolving. To understand how things stand in your market and for your particular project, you **could**:

- conduct competitor analysis to understand how others are positioned and look for ways to compete or differentiate by enhancing privacy;
- explore emerging technology or industry trends that could offer novel ways of tackling privacy challenges; or
- review any consumer trends that are shaping the privacy landscape, and identify how to investigate these more deeply in your own research.

14. Gather audience perspectives on privacy

Researching people’s attitudes towards privacy means you’re less likely to violate their expectations. ‘Formative’ research such as focus groups, interviews, diary studies, and citizens’ panels can help you learn how different groups feel about privacy and personal information use in your product. Questions you **could** explore in research include:

- Who will use the product? Do they include children or vulnerable groups?

- How might the collection of personal information affect them?
- What risks might there be in collecting personal information for different people using the product?
- Would people expect you to use their information in this way?
- When in your user journey do people need to understand how their information is used?
- How can you design that information in ways people can understand and engage with in the context of your product's user journey and people's state of mind?

If time and budget allow, you **could** also use participatory methods, such as co-designing critical interactions with representative users.

Findings about people's views on privacy and personal data might feed in to any data protection impact assessment that you or your data protection and legal colleagues complete.

15. Get feedback on privacy work in progress

You **could** also conduct 'summative' research to test work in progress and see whether you are on the right track:

- Assess the design of privacy information screens, consent interfaces and flows, and other data interactions, just as you would for other elements of your product experience.
- Test whether people can easily access and understand relevant privacy information, whether participants feel they have the right information at the right time, and whether they are in the appropriate state of mind to take informed action.
- Recruit a representative sample of your intended users for tests; you may find different people have significantly different privacy needs and reactions.

16. Protect the privacy of your research participants

Conducting research ethically and properly means taking participants' privacy seriously. If your research requires you to process personal data, you **must**:

- minimise the information you collect about your participants. You **should** anonymise results where possible. You **could**, for example, refer to each participant just by a number rather than a name;

- clearly explain to participants how you will collect, store and use their information;
- ask for participants' consent for data processing when appropriate, and keep records of this consent; and
- erase or anonymise participants' personal information in the time period you specified. You must not keep personal information for longer than you need to.

• Design

Share(Opens Share panel)

Whether sketching initial design concepts, planning out user journeys, or prototyping high-fidelity interactions, you **must** consider privacy throughout your design process. It is easier to resolve issues in a design phase than if you discover them later on.

17. Consider privacy throughout your design activities

You can address privacy issues through a range of design activities, including UI sketching, information architecture, prototyping, and content design:

- You **could** try using privacy concepts as a prompt for generating ideas, such as a 'crazy eights' sketching exercise that explores how your product might work if it processed no personal information.
- You **should** avoid using real user data when prototyping or mocking up interfaces. Realistic dummy data or synthetic data is safer.
- Critique sessions offer good opportunities to ask what-if questions about privacy. You **could**, for example, use the ICO's Overview of data protection harms as a discussion prompt.
- If you are a design leader, you **should** make it clear that designers should consider privacy in their work. You **could** also specify that you will not sign designs off until the team shows how they have handled privacy questions.

18. Communicate privacy information in ways people understand

You should design experiences that allow people to understand what happens to their personal information, to help meet the requirements of the UK GDPR's transparency principle and people's right to be informed:

- Privacy information should be easy to read and understand. You **must** make it concise, transparent, intelligible, easily accessible, and use clear and plain language.

- People may not always read privacy notices. It may not be sufficient to only use this way of communicating privacy information. You **should** use a variety of techniques such as ‘just-in-time’ notices or a layered approach, where appropriate.
- Your users may not understand technology and privacy as well as you. Remember that the consequences of decisions may not be obvious to others, even if they are to you.

Example

A young man, excited to have his first credit card, tries to post a photo of it to social media, unaware that sharing card information could expose him to fraud. The social media company uses an image recognition algorithm to scan for possible credit card photos, and intervenes in the posting flow, advising the user not to post his sensitive financial information. Although this safeguard is not legally required under data protection law, it helps to protect people.

- You **should** recognise and respect use cases that don’t fit your ideal user journey.

Example

A designer working for a ride-hailing service believes the best pickup experience involves users sharing their device location. However, some people will decline to share, as is their right. The designer realises these are not edge cases and designs a smooth, accessible way for them to enter a pickup location, using either text or voice input.

Further reading

- What methods can we use to provide privacy information?

19. Choose the right moments

Timing is everything. You **should** identify the moments when people might expect to make decisions about information, and when they are in the best state of mind to make reasonable, informed choices:

- Consider when in the user journey you should discuss privacy. You **must** provide privacy information at the time of collecting personal information from the person it relates to, but consider additional moments.

Example

A design team is unsure whether to explain what happens to people’s information through step-by-step instructions during initial account sign-up, or as ‘just in time’ prompts before information is

collected later on. Since the team agrees it is important that people fully understand what happens to their information, they opt to do both.

- The right moments may vary for different people with different needs.
- Whatever moments you choose, you **should** ensure people have enough time and knowledge to consider their options fully.

20. Ensure consent is valid

Consent is one of six lawful reasons for processing personal information. Your data protection colleagues can advise you about whether you need to seek consent for your use case. Consent must be freely given, specific and informed, and given by a clear affirmative act. It must represent an active choice and be as easy to withdraw as it is to give.

How you present choices in an interface can help people make better decisions, but it can also affect their actions and invalidate their consent:

- You **must** offer consent interfaces that are unambiguous and involve a clear affirmative action (an opt-in). Pre-ticked opt-in boxes are specifically banned under UK GDPR.
- You **should** think carefully about when to use consent interfaces. Use too few and you may not comply with UK GDPR requirements, if you are using consent as your lawful reason. However, over-using unnecessary consent popups causes decision fatigue, training people to accept information sharing or other uses of their information blindly in every product they encounter.
- You **must** offer people a way to reopen consent interfaces later on. It must be as easy to withdraw consent as it is to give it.

Further reading

- What is valid consent?
- When is consent invalid?

21. Empower people to exercise their information rights in the interface

The UK GDPR gives people various rights about their personal information. These rights include:

- right of access – people have the right to get access to their personal information, and should be able to request a copy;
- right to rectification – people have the right to request that inaccurate information is rectified, or that incomplete information is completed;
- right to data portability – people have the right to move, copy or transfer personal information easily from your product to another, in a safe and secure way; and
- rights related to automated decision-making and profiling.

Your organisation **must** allow people to exercise these rights. Since it is good practice to provide privacy information through the same medium used to collect it, you **should** consider how you could help people exercise their rights directly through your product.

Example

A credit agency allows people to request corrections to their personal records by email and post. However, these channels create high administration overheads and are expensive. The agency's web team therefore builds an online form to let people request corrections themselves, and additionally to download their data in an interoperable format.

Further reading

- Individual rights
- Information rights bingo tool – check whether your product lets people exercise their information rights.

• Development

Share(Opens Share panel)

You **must** carry forward your privacy planning from previous stages all the way into the finished product or feature. Careful privacy engineering makes systems more reliable and protects people.

22. Define the minimum personal information you require

You **must** only collect the personal information you really need. The more information you handle, the greater the data management overheads and potential privacy risks.

You **should**:

- review any data maps you created during kick-off, and check you are using the minimum personal information you need to make the product or feature work;
- clarify what the feature or product is trying to achieve and double-check whether you really need personal information to achieve your outcomes;
- question any personal information collection that seems unnecessary and raise it with your data protection officer or legal colleagues. If the processing isn't necessary, it may be unlawful; and
- check that people can access as much functionality as possible without having to provide personal information.

Further reading

- Principle: Data minimisation

23. Enhance privacy and security with technical measures

Proper security engineering protects people from privacy harms. You **should**:

- store private, sensitive, or secret information like usernames, passwords, and cryptographic keys securely. You **should not** store passwords in plaintext;
- use hashing, encryption, or other privacy-enhancing methods to protect information in storage, backups, and in transit;
- consider how you could use novel architectures for information handling, such as federated, decentralised, or on-device processing to enhance privacy and security.

Example

The makers of a mobile OS offer voice recognition functionality. Previously, this has involved processed speech audio being sent to centralised cloud systems for processing. Now, speech snippets are processed directly on a user's handset and converted into text strings that are interpreted by the OS itself.

- offer people enhanced security options such as two-factor authentication, where appropriate, to help people stay secure. If your product uses default passwords, you **should** design ways for people to replace these with secure passwords of their choice.

Further reading

- Passwords in online services
- Privacy-enhancing technologies draft guidance (PDF)

24. Ensure people can exercise their data rights

People have a range of individual rights under UK GDPR. Any organisation processing personal information must ensure these rights can be exercised:

- As discussed in the design phase, you **could** consider letting people exercise these rights directly through your product.
- You **must** ensure people can enter their personal information accurately and request amendments through the right to rectification.

Example

A developer building a health-tech product takes extra care to ensure name input fields accept accented characters and non-Western name formats. They also review database fields that store people's heights and weights, and removes unreasonable limits on what values the system considers valid, so people outside these ranges can have their personal information recorded accurately.

25. Protect personal information during development

Your organisation **must** process personal information securely by ‘appropriate technical and organisational measures’. To do this, you **should**:

- set up proper access control systems so other people (including internal users) can only access the information they need to see;
- consider logging data interactions, such as who has accessed or modified data;
- establish retention policies so you aren’t holding onto information beyond its proper lifespan;
- check all third-party libraries you use are secure and not likely to leak private information;
- embrace QA or code review processes so teammates can verify your code is secure and free of vulnerabilities; and
- understand where adversaries might try to attack your system, and take steps to reinforce any vulnerable areas.

You could also choose to follow established secure coding practices, such as the National Cyber Security Centre’s Secure development and deployment guidance and OWASP’s Secure Coding Practices Quick Reference Guide.

• Launch

Share(Opens Share panel)

You’re almost ready to share your work with the world. Before you do, check you’ve addressed any lingering privacy issues.

26. Check carefully before release

Are you confident you have mitigated any privacy risks identified in earlier stages? Unresolved concerns can lead to legal risks and harm customers’ confidence.

- You **should** check with legal, data protection, and other senior stakeholders that they are happy for your product or feature to launch.
- If you are unsure whether people’s privacy needs are fully met, you **could** conduct a round of usability testing focusing on privacy, to assess your solutions (see Research).
- Bugs are often dangerous sources of privacy issues. You **should** run regression tests to check whether the new feature has broken old code.
- As you launch to live environments, you **should** remove or replace test or staging data.

27. Factor privacy into rollout plans

If you have a launch checklist, a few points about privacy could save a lot of trouble after launch:

- You **should** plan what to do if something goes wrong. Do you have a rollback strategy, or another way to fix problematic code? If you face an issue that affects people’s access to personal information, your organisation **must** ensure this access is restored in a timely manner.
- To help respond to new customer feedback and privacy-related questions, you **could** inform your customer support team of changes you’ve made before launch.
- How will you get early warning of any privacy issues once you launch? You **could** look, for example, for evidence of younger people accessing the feature, reports of harm, or analytics that suggest people are accessing reporting or support interactions. If this analysis involves

storing information on a user's device, or accessing information stored on a user's device, you **must** obtain consent for this analysis.

Example

The makers of a dieting app are launching a new integration with a fitness app run by a partner company. The project team makes plans to monitor customer feedback on forums for three months after launch, and to track data on how many people choose to use the feature.

- You **should** build in some time after launch to identify and fix any issues that emerge.

28. Tell people what to expect

Under UK GDPR, people have the right to be informed about how their personal information is processed. For example, if your new product or feature affects how you collect or use personal information, you **must** provide clear and understandable information on these changes.

- To explain the privacy aspects of new features, you **could** use product marketing, release notes, or in-app communications. Describing the protections you've put in place helps ease people's concerns, leading to greater trust and adoption.
- You **could** also tell people of any new behaviours you recommend they adopt to reduce the risk of future privacy problems, such as enhanced password management practices.

• Post-launch

Share(Opens Share panel)

The launch is not the end of the journey. It’s now time to review how people are using your work, and to consider whether you need to make fixes to protect people and their information.

29. Monitor and fix as required

After launching your product or feature, you **should** examine whether any unexpected privacy issues have arisen, and prioritise any remedial work if so:

- In the event of serious privacy problems, such as a suspected personal data breach, you **must** consult data protection or legal colleagues immediately. They may need to begin formal processes straight away.
- You **could** check how people engage with your product’s privacy information and data choices. If appropriate, use analytics to quantify these interactions. Try to minimise the data you collect in this work, and note that you may need people’s consent for some of this analysis.

Example

An e-commerce company is offered third-party customer tracking software that allows them to monitor a person’s mouse movements. The team declines this on privacy grounds, and chooses instead to simply analyse aggregate data on how many people visit various parts of the purchase funnel.

- You **could** also look for qualitative data, including feedback from people through social media, support forums, or customer services.
- You **could** also look for feedback from non-users and communities who might still be affected by your product.

Example

A new augmented reality game involves sharing photos of local neighbourhoods. The team realises this may impact privacy expectations of their players’ neighbours. The game designers therefore consult community representatives before and after launching in a new region, to understand any concerns and to integrate this feedback into future iterations.

Further reading

- Personal data breaches

30. Reappraise expectations and norms

Each new release can change how people understand and interact with your product:

- If new features significantly affect people's privacy expectations, or introduce new privacy risks, you **must** review these and take them into account in the next feature or iteration.
- If you see significant new behaviours after launch – particularly behaviours you didn't expect – you **should** assess any emerging privacy implications.

Example

A team has recently launched a new video sharing platform. Follow-up research reveals the product is particularly popular with under 18's. The team had designed the product for adults and not considered privacy risks to children as outlined by the Children's code. This post-launch data triggered a privacy review which found several privacy risks to children that needed to be resolved immediately. The team proposes new features to mitigate the risks, and the product design lifecycle starts again.

31. Reflect, celebrate, and improve

Retrospectives or project reviews can help you learn from how you handled privacy topics. You **could**, for example:

- discuss any privacy challenges you faced. What went well? What could have gone better? Are there habits or processes you should start or stop, to improve things for next time?; and
- celebrate privacy successes with your team. Did you identify and mitigate a potential problem before it went live? Get the credit you deserve by discussing your success in demos, and reports, and encourage others to make privacy consideration a repeated habit.