Guest columnist

OLIVIA WHITCROFT

"How do you launch a product without alienating or damaging your customers?"

Data protection by design isn't a buzz phrase for companies to ignore. It's a principle that should guide you on every step of a customer's journey

Let me tell you a story: you're having a new friend round for lunch. You've designed a recipe for "Meaty Platter", which combines a range of meats. You've bought the finest ingredients for the platter. That morning you blended it together and made it look amazing. Your friend arrives. She takes one look at your beautiful platter and declines to eat it; she doesn't understand what it's made from, and doesn't want to eat meat. Meaty Platter goes in the bin, and your friend doesn't return. Or maybe she takes a taste, and then suffers a severe stomach ache later that day, and your friendship is lost.

So how do you host a lunch without alienating or damaging your friends?

Before designing your recipe, you consider whether aspects of your menu may use ingredients unsuitable for some guests. You could also ask your guests if they have any dietary concerns. Any issues can then be addressed within your recipe. You can prepare a tailored platter with all dietary needs baked into it. You can let guests know what it is, so they can make an informed decision whether to eat it. In my story, you could then present your friend with a meal she understands. Meaty Platter (perhaps renamed to Veggie Platter) hopefully won't be thrown in the bin. If your friend takes a taste, she is less likely to suffer a stomach ache, and you're more likely to retain your friendship.

You may not be able to eliminate every risk. You are unlikely to have considered all potential eventualities, or to have discussed with every guest the full detail of your menu. A guest may have an unforeseen dislike to a particular ingredient, or a previously unknown allergy. But, by considering the risks in advance, and without taking disproportionate steps to guarantee a fault-free meal, you have minimised the risk that a dietary issue leads to your food not being eaten or causing damage to your guests.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"Without data protection by design, data protection may only be an afterthought"

The story retold

Let me tell you another story: you're launching a new technology product. You've designed a recipe for "Meeting Platform", which combines a range of information about customers' online habits, to create the perfect meeting experience. Over the past year, you've engaged the finest coders for each component of the platform. You have been blending it all together and making it look amazing. You press the launch button (there's always a big launch button, right?), and your customers enter your platform. They take one look at your beautiful product and decline to use it; they don't understand what you do with the requested data, and they don't want to provide it. Meeting Platform is shelved, and your customers don't return. Or maybe some customers take a taste, and then you suffer a severe security breach later that week, and customer data is lost.

So how do you launch a product without alienating or damaging your customers?

Before designing your product, you consider whether aspects of it may use personal data. You could also ask potential customers if they have any concerns with the use of their data. Any issues can then be addressed in the recipe, and the components that form part of it. You can prepare a tailored platform with data protection needs baked into it. You can let customers know what you'll do with their data, so they can make an informed decision whether to use it. You can then present customers with a product they understand and want to use. Meeting Platform hopefully won't be shelved. If your customers take a taste, you're less likely to suffer a security breach, and you're more likely to retain your customers.

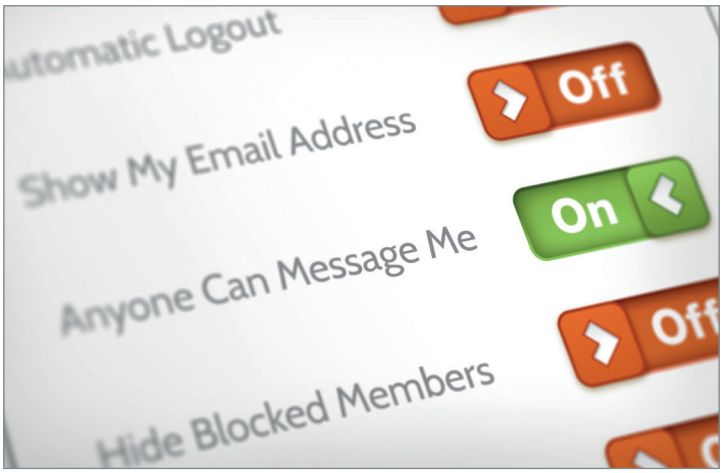
You may not be able to eliminate every risk. You are unlikely to have considered all potential eventualities, or to have discussed with every customer the full detail of the platform's use of personal data. A customer may have an unforeseen dislike of a particular use of data, or the system may have a previously unknown vulnerability. But, by considering the risks in advance, and without taking disproportionate steps to guarantee a fault-free product, you've minimised the risk that a data protection issue leads to your product not being used or causing damage to your customers.

Data protection by design

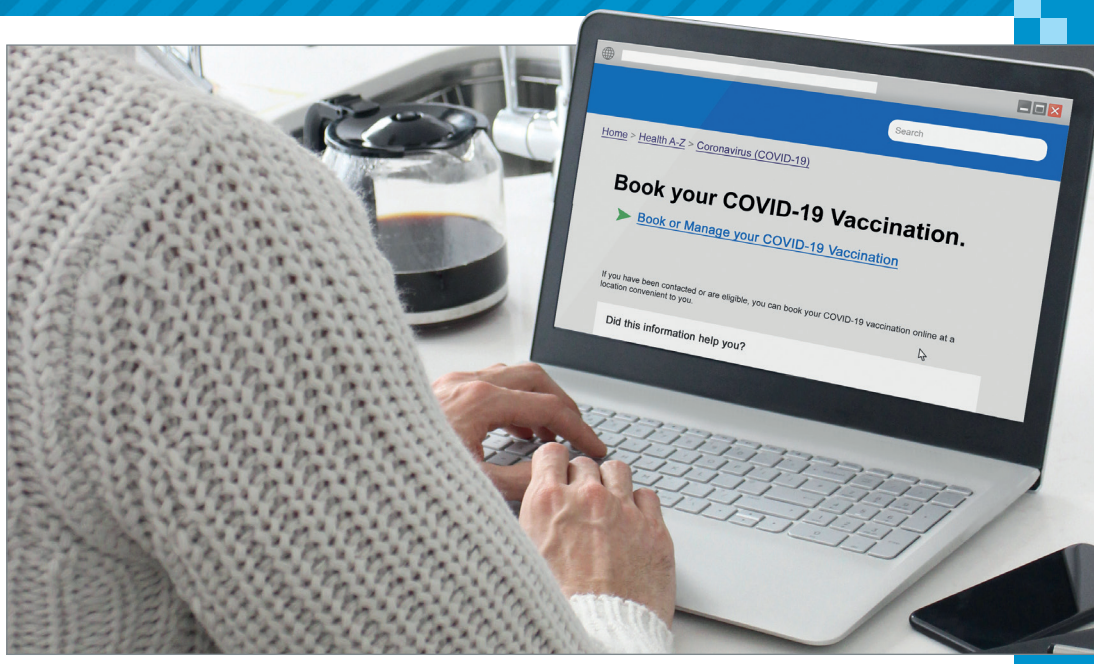
Data protection by design is just this. It is about baking in data protection compliance into the design and development of new activities involving the use of personal data. All data protection requirements should be addressed, including the core principles (such as transparency, data minimisation and security) and enabling individuals to exercise their rights (such as to access and erase data).

Data protection by design is a legal requirement under Article 25 UK GDPR, along with the closely related concept of data protection by default. This requires that the default position for any activity is to collect the minimum amount of data and do the minimum amount of processing. The obligations are ongoing throughout the lifecycle of the use of data.

Without data protection by design, data protection may only be an afterthought for a project (by which time it may be too late to address issues), or it may be ignored completely. This may lead to the project



BELOW **Give potential customers as many options as possible about the use of data**



being shelved. As a topical example, the NHS Covid-19 app faced several data protection hurdles. Privacy concerns were key to the government scrapping the original 2020 model. And in 2021, it was reported that an update to the app had been blocked by Apple and Google due to prohibited collection of location data.

Even if a project isn't cancelled, it could cause significant costs and delays to rework it to address data protection issues. In May 2019, the Information Commissioner's Office (ICO, the UK data protection regulator) issued an enforcement notice against HMRC in relation to its Voice ID service, requiring it to delete data. The ICO found that HMRC was processing biometric data (for voice authentication) without a lawful basis under data protection law, as it had failed to obtain adequate consent. In its notice, the ICO stated: "HMRC appears to have given little or no consideration to the data protection principles when rolling out the Voice ID service." In other words, it didn't apply data protection by design.

When is it needed?

Data protection by design most obviously springs to mind for big projects, such as new technology systems that will process personal data. However, its remit is much wider than this. It applies to all activities involving personal data, big or small, and to the preparation of policies and processes that govern the use of data. However, you may not need to carry out the same level of review in each case. As raised in my stories, the approach you take and the extent of measures you put in place should be proportionate to the risks involved.

Consider, for example, a business's use of customer contact details to keep customers updated about requested services. Design measures may include ensuring customer details aren't used for a wider purpose, and are kept up to date and secure from misuse. However, the assessment may be fairly quick, and the measures fairly standard. Compare this with more innovative or intrusive uses of data, such as those involving artificial intelligence or sensitive data, or monitoring and profiling individuals. A more complex assessment and more bespoke design measures are likely to be needed. For these types of higher risk activities, a formal data protection impact assessment (DPIA) may be needed (under Article 35 UK GDPR), and a DPIA forms an important part of data protection by design. Consultation with data subjects (in other words, asking those who will be impacted for their views), is also a stage of the DPIA process.

In my experience, higher-risk projects are commonly now given some quality data protection time. However, I still come across some clangers. Just the other day, a company sent its employees a request to provide their Covid-19 vaccination details, together with proof of vaccination (with type of vaccine and dates), or the reason why they were unvaccinated. The request had no explanation as to what would be done with this information. My head started firing out data protection principles: there was no transparency or specified purpose! What was the lawful basis? How about data minimisation?

At the lower-risk end of the spectrum, I find there is a tendency to focus on specific aspects of compliance (such as having a privacy notice, and checking security measures), without looking at the full range of data protection design elements. As an example, one of my clients recently launched a new website, and included a form for people to sign up to receive a newsletter. However, there was no newsletter – this request was "just in case" the company decided to create one in the future. Data protection by default, and the principle of data minimisation, would say don't collect this information yet, as it isn't needed right now.

ABOVE The NHS is just one organisation to fall foul of data protection concerns

"Data protection by design applies to all activities involving personal data, big or small"

BELOW Never ask users to provide details you don't actually need

Raising PETs

The organisations actually collecting and handling personal data have legal responsibilities under data protection law. However, product developers have a role in designing systems with data protection embedded, which can also be a selling point for them. This is the aim of "privacy-enhancing technologies", meaning technologies that are designed for supporting specific privacy or data protection functionality, or protecting against privacy risks. They are currently a hot topic in the data protection world.

I have excitedly been trying to understand mathematical concepts such as differential privacy (adding "noise" to statistics to make it more difficult to identify source data), and homomorphic encryption (which enables functions to be carried out on specific data without decrypting whole data sets). Anonymisation and pseudonymisation functionality can also be built into technology design. These types of measures may most obviously assist with information security, but they have wider data protection benefits. They may, for example, limit retention periods by ensuring that individuals can no longer be identified from data sets; ensure that only the minimum amount of personal data is held within a system; and facilitate the exercise of rights by data subjects.

So next time you're designing your recipe for new technology or data-processing activities (or even a meaty platter), don't forget to bake in your data protection (or dietary) requirements.

olivia.whitcroft@obep.uk