Deloitte.

Customer Breach Support

Decoding the data controller and processor relationship in a data breach

Introduction

Your phone rings and you hear the words you have dreaded for so long: “We’ve had a data breach.” Only it is not your Chief Information Security Officer calling, but rather the General Counsel of the major data processor supporting much of your business — maybe payroll, customer invoicing or IT. For a moment relief breaks out. But then reality sets in. This could be even worse than your own breach.

So, what happens if your data processor has a breach? From our experience, very few businesses conduct tabletop exercises with their processor to discuss and agree in detail how they would handle a data breach. Certainly, few companies have crisis plans that define how the data controller and processor will operate together.

When sensitive data has been lost and may be in the hands of cyber criminals, the next target will be the actual data subjects; whether that is for a spurious phone call scam or to hack into their online accounts. This is the real race. The sooner customers know they are at risk the sooner they can take action to protect themselves, so quick notification is vitally important.

Understanding clearly who will do what, how and when is key to the delivery of a successful data breach response and ensuring the protection of your customers, not to mention your brand and reputation.

Who is responsible?

A 'data processor' is an organisation that processes data. ‘Processing data’ is defined as any action performed upon personal data by a business. The ‘data controller’ is the business that determines the purpose and means of processing the data. When a data controller engages an external business to conduct data processing, that business becomes the data processor.[1]

The controller is well and truly responsible for the integrity and confidentiality of the data that is entrusted to them. At the same time, under General Data Protection Regulation (GDPR), the processor is required to apply the same diligence as controllers.[1] Thus, by law, there is a virtuous circle of protection that must be provided to the data subject.

[1] Article 4, General Data Protection Regulation (EU) 2016/679

Notifying the regulator

Article 33 in GDPR is very clear on the requirements placed upon the data controller, so far as notification of a data breach is concerned:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."[2]

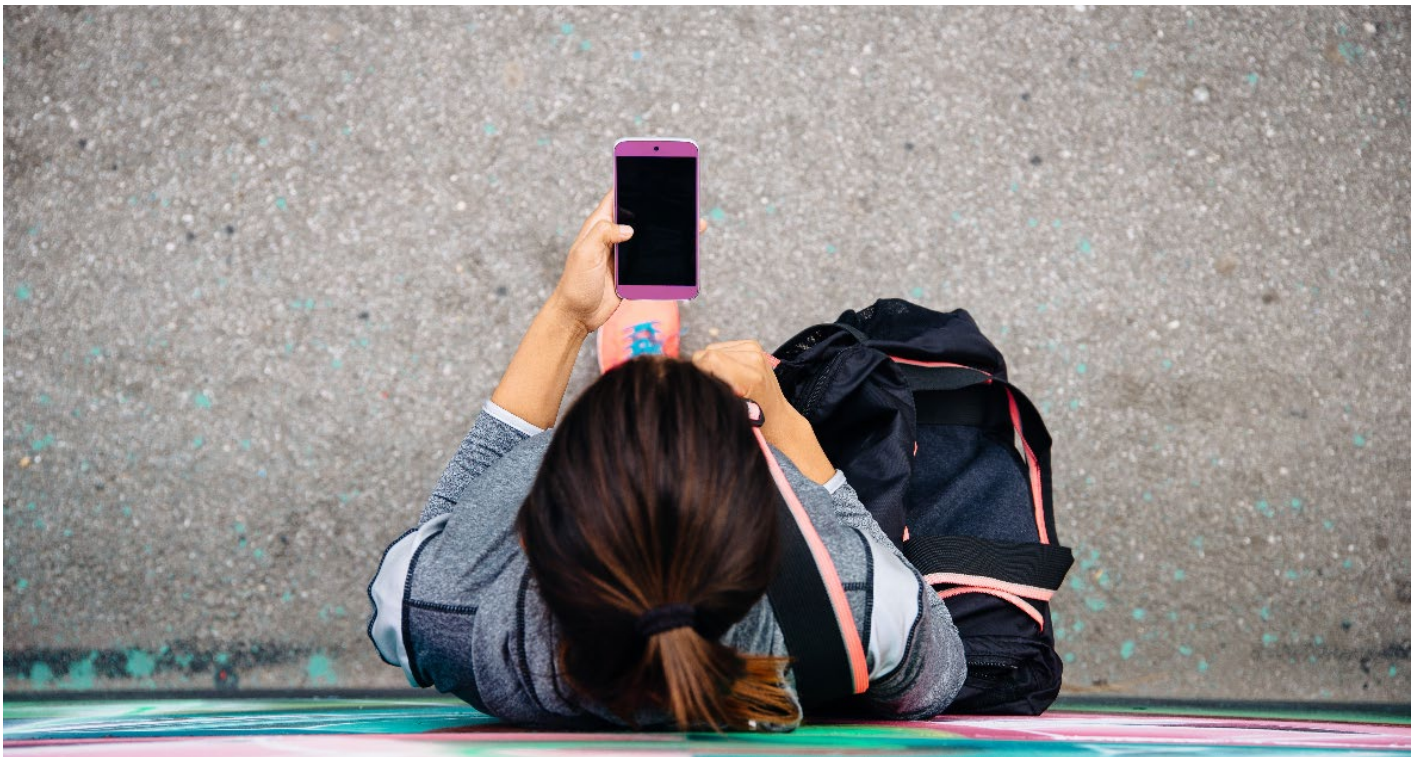
However, the regulation becomes much less clear so far as the data processor is concerned:

"The processor shall notify the controller without undue delay after becoming aware of a personal data breach."[2]

Under GDPR, the processor responsible for losing the controller's data only has to inform their controller "without undue delay." As a result, controllers can face inbuilt delays when responding to breaches. Of course, well prepared processors will act promptly but the subjective "undue" term will inevitably lead to some issues. In addition to this, naturally, processors are likely to have a number of clients on their books, meaning they will have many organisations to support. Together, these factors make matters complex. To combat this, controllers must clearly outline what they expect from their processor in the event of a data breach.

[2] Article 33, General Data Protection Regulation (EU) 2016/679

Who is going to notify your customers?



When a data processor has a data breach, under GDPR, they are not "required" to notify affected customers. Technically, that responsibility sits with the data controller. This situation could be complicated further if under normal circumstances, the controller relies on the processor for customer notification.

The next question is whether your processor has the means to notify your customers effectively — whether it be by email or post. Then you have to deal with the surge of customer calls that could overwhelm your contact centres unless you have robust plans in place.

When drawing-up contracts that cover all the technical needs of GDPR, it is also key to address how the processor will support you in the critical stages of a breach response — particularly if they have wider problems to deal with, such as containing the breach and managing many other clients. Roles and responsibilities for notification and support should be made clear, along with an agreed approach for building breach response plans and running regular exercises to test those plans.

During a data breach of a large amount of customer data, the notification of those customers is your responsibility.

The notification process

When a data processor experiences a breach, their reputation is not the only one on the line. The general public will not care about the commercial relationships and may well see this as a breach of the data controller. The brand issue is key in this complicated phase. Whose website will say what, and which logos will be on the notification letters or emails?

Following notification, there will be an influx of calls from customers seeking to understand what has happened and what precautions they should take. Dealing with a prolonged surge in calls would be challenging for any business, but it will be an even greater test for smaller businesses and organisations with a large customer database relative to their operational capacity (e.g. pension fund managers or financial services challenger entities). As the source of a data breach, should processors provide contact centres for their controllers or pay for such provisions?

It is clear that at a point of operational crisis, the controller-processor relationship is one that must be fully understood and supported by comprehensive agreements and associated capabilities. This will ensure that customers get a fast and effective response that supports and protects them — a key step in preventing avoidable damage to reputation and potential litigation claims.

The cost and operational complexity of dealing with a breach by a data processor

When a data processor is impacted by a data breach, which affects multiple data controllers, there are three questions relating to cost and complexity that need to be addressed:

1. **Who picks up the costs, across processor and controllers, of dealing with the data breach?**
   - Commercial arrangements between controllers and processors should ensure that the burden rests with the processor who experienced the breach, but these arrangements need to be verified.
   - It will also be important to ensure that liability caps are appropriate, if not unlimited, to ensure that costs do not hit the controller.
   - Controllers must ensure that their insurance policies cover the cost if processor liability limits are exceeded.
   - Processors must ensure that their insurance policies cover contractual liabilities, noting that insurers will only cover costs that are insurable by law.

2. **How do you minimise complexity to ensure that customers receive the best service?**
   - Should each controller take the lead in dealing with their own customers (using their own service providers), or should the processor lead the customer support activity?
   - If the processor leads, how do the controllers ensure that brand and service levels are appropriate for their impacted customers?
   - A controller-led approach will certainly be more complex, involving far more third parties and suppliers. Whilst brand owners may want to control all customer interaction, will the increased complexity and cost of full data controller ownership ultimately impact the customer experience?

3. **What is the overall lowest cost route for delivering customer breach support?**
   - The lowest cost solution will generally follow the simplest operational solution, but will the interests of insurer, processor and controller align here? What flexibility will the various insurance policies and carriers provide?
   - Open communication, advanced planning, preparation and practice will be key to ensuring that the overall economic cost of the breach is managed effectively, whilst also delivering a high-quality service to the people who need it most: the customers.

Conclusion

GDPR clearly lays out the requirements placed on data processors and the expectations on data controllers to assure standards are met. As ever, with situations such as data breaches, clarity of responsibilities will be key in doing the right thing for customers who can easily be forgotten.

Controllers need to get together with their processors to ensure there is complete clarity over who will do what, where the costs will lie, and how the joint operation will function — including how key decisions will be made. When news of a data breach hits, disagreements and delays are the last thing that anyone needs, whether controller, processor or impacted customer. Both the controller's and processor's reputations will be on the line. To recover from the blow of a breach, organisations must demonstrate a well-considered, fully resourced and professionally delivered response in order to provide an outstanding customer experience, whatever the circumstances.

Get in touch

Hugo Morris

Partner

Risk Advisory

+44 (0) 20 7303 5985

hmorris@deloitte.co.uk

Mark Whitehead

Director

Risk Advisory

+44 (0) 20 7303 0698

marwhitehead@deloitte.co.uk

Deloitte.