Identifying the harms and impact of a personal data breach

February 2024

Contents

1.1 Introduction

This report presents the findings of a project which explored the impact and data protection harms that may occur when people experience a personal data breach. Written for internal publication, the report aligns with our strategic enduring objectives as defined by ICO25, including Objective one "safeguard and empower people particularly the most vulnerable"[1]. Fundamental to the delivery of the report was collaboration with colleagues across the office, specifically with the Personal Data Breach Service (PDB). Organisations are required to notify the ICO of a breach if it is likely to result in a risk to the rights and freedoms of individuals. During 2021-2022, over 9,500 data security breach reports were received by PDB, who are the first point of contact for organisations. Their responsibilities include advising organisations on steps they should take to mitigate risk and avoid future incidents occurring.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The report shares case examples where people were adversely impacted by data breaches – and demonstrates how a simple error has the potential to cause long-term harm, particularly for those most severely impacted by the breach.

This report is aimed at colleagues across the office who are delivering workstreams/ have a specific interest relating to the ICO's commitment to safeguard and empower people - particularly those at the greatest risk of harm. It comes at a time where the ICO is considering how resources and interventions should be focused, to have the greatest impact. Within the report, we provide examples of how people have exchanged their privacy for the purpose of accessing specialist services and we consider ways to empower organisations to use information more responsibly, so that people can confidently share their personal data.

An initial scoping exercise for the project considered the impact and data protection harms that data breaches have on people and follows on from information gathered during 2019/ 20 (as explained below in 1.2 Background). Using the policy methodology framework, the project team identified how best to discover and analyse relevant evidence, before determining recommendations and next steps. This involved scrutinising 98 breach reports and interrogating the contents using a series of questions devised using MS Forms. The recommendations include:

- developing guidance for those organisations who are likely to process the data of people most likely to experience harm following a data breach;

[1] See section 1.2 Regarding 'vulnerability'

- identifying additional ways to recognise cases where a breach has made a person 'vulnerable'; and
- improving internal systems and processes so that cases/ incidents involving those at most risk of harm can be recorded, measured, monitored and shared with relevant colleagues across office.

1.2 Regarding 'vulnerability'

At the start of the project, we based our understanding of 'harm' on the definition of vulnerability developed at the time by the Vulnerability Working Group, which states:

The ICO defines a vulnerable individual as someone who due to their needs or personal circumstances is especially susceptible to harm or detriment, which may impact their information rights. The ICO recognises that everyone is at risk of harm from misuse of their personal data, but this risk is increased by having characteristics of vulnerability. This definition is intentionally broad, to include both permanent and temporary (circumstantial) vulnerability (for example, permanent capacity concerns due to a learning disability, or temporary vulnerability due to a period of unemployment), and also includes those at risk of inequality.

We acknowledge the shift of approach regarding 'vulnerability' during the lifecycle of the project and recognise that our Style Guide has been updated, to ensure the ICO promotes inclusive language and avoids further victimisation of people. We also note that a Communities Working Group has been set up, to progress this approach across the office. This scrutiny of what we mean by vulnerability reflects its importance to the ICO. Throughout the project, we have focused on where harm has been caused and have based our recommendations on where we have discovered evidence of harms/ potential harms.

1.3 Background

In 2019, case examples demonstrating breaches of personal data involving people at most risk of harm were collated within the PDB department and shared with Intelligence colleagues. A Tactical tasking and coordination group (TCG) was subsequently commissioned to determine the most effective way to consider this matter and at the time created a definition of a vulnerable individual as *'someone who due to their needs or personal circumstances is especially susceptible to detriment, which may impact their information rights'* (strategic assessment September 2020). In addition, the strategic assessment

described the psychological impact on victims of domestic abuse who were required to relocate, following a disclosure of their address. This was echoed in a report published by Citizen's Advice (CA) in February 2020, entitled On the receiving end which described the significant harm faced by survivors of domestic abuse, because of addresses being regularly disclosed. This is a common form of a data breach with the potential for a catastrophic impact on people. In their report, CA uncovered a range of issues including:

- 71% of those who had their new address disclosed by an agency said their safety was compromised as a result; and
- 51% of those who left an abusive home avoided engaging with essential services, as they didn't feel comfortable sharing their new address.

CA provided recommendations for the ICO, including the need to "investigate the significant number of data breaches highlighted by their research". The report was published just before the start of the Covid pandemic and while brief conversations were held with CA to discuss their findings, no further action was taken regarding their recommendations.

More recently, this project was approved to explore the impact and data protection harms which data breaches have on people. The team was comprised of policy project colleagues who had previously worked in PDB for a combined total of nine years, and an experienced colleague from PDB who collaborated with the rest of the PDB team and provided insights on current delivery. Objectives included:

- gathering evidence to determine the prevalence of this issue;
- identifying the impact and harm/ potential harm to those who experienced a data breach;
- developing an understanding of the internal systems and processes used by the ICO; and
- making recommendations based on our research which might influence positive outcomes for those who are affected by a data breach, and identify ways to reduce the likelihood of breaches occurring.

The project developed at a time where the strategic enduring objectives determined by ICO25 had been progressing for the past 12 months. Aligning with ICO25 priorities, our findings demonstrate the need to support proposals which include levelling the power balance between those who hold data and those who hand over their data, and providing additional support and guidance to the public, businesses and organisations.

2.1 Internal and external discovery

The project engaged with departments across the ICO on a range of matters. Initially, we wanted to build evidence on the prevalence of this matter (based on reported cases). This was followed by understanding the internal systems and processes used to identify and respond to cases involving those at risk of greater harm. Further, we considered the information provided by the ICO to customers, organisations and the general public.

Internal engagement included:

- Personal Data Breach Service colleagues, to inform them of the project, to discuss PDB systems and processes and to provide progress updates. Collaborating with PDB was crucial to the project and enabled access to a member of this team, who provided insights to current processes;
- Public Advice and Data Protection Complaints Service (PADPCS), to understand what links there might be between a breach reported to the ICO by a controller and a complaint reported by a customer;
- Civil Investigations, to find out how a reported breach might be referred for further scrutiny by them, what this process entails and to discuss aspects of specific cases;
- Public Affairs - Sectors, to determine what the engagement with CA had been, following the publication of their report;
- SME hub, to discuss guidance available for small organisations.
- Economic analysis, to identify and consider the harms experienced by people when their personal data had been compromised; and
- Data services team, to discuss the functionality of ICE360 (an internal case management system).

External engagement:

As it had already highlighted concerns around the disclosure of personal data, the starting point for external engagement was with CA. It shared information about the background to their report, the methodology used and what the expectations were of those involved in the research.

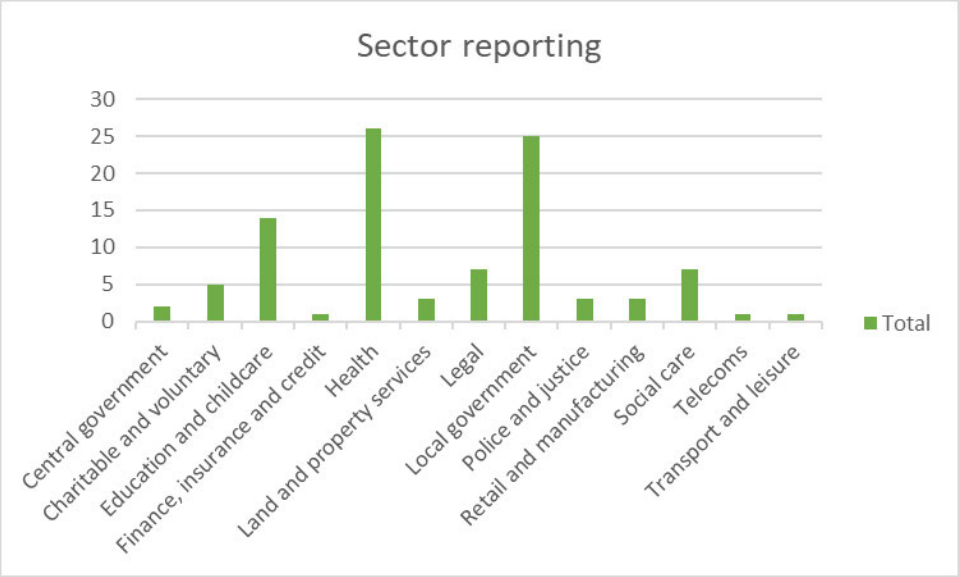
CA suggested we also engage with Surviving Economic Abuse (SEA). This is a third sector organisation that has provided advice and support to a range of financial organisations on how to better protect the personal data they hold about on customers who have experienced domestic abuse. SEA shared information about systemic issues within some organisations that result in breaches occurring and explained how they have developed an 'experts by experience' group, who provides insights into the lived experiences of victims-survivors.

3.1 Methodology and limitations

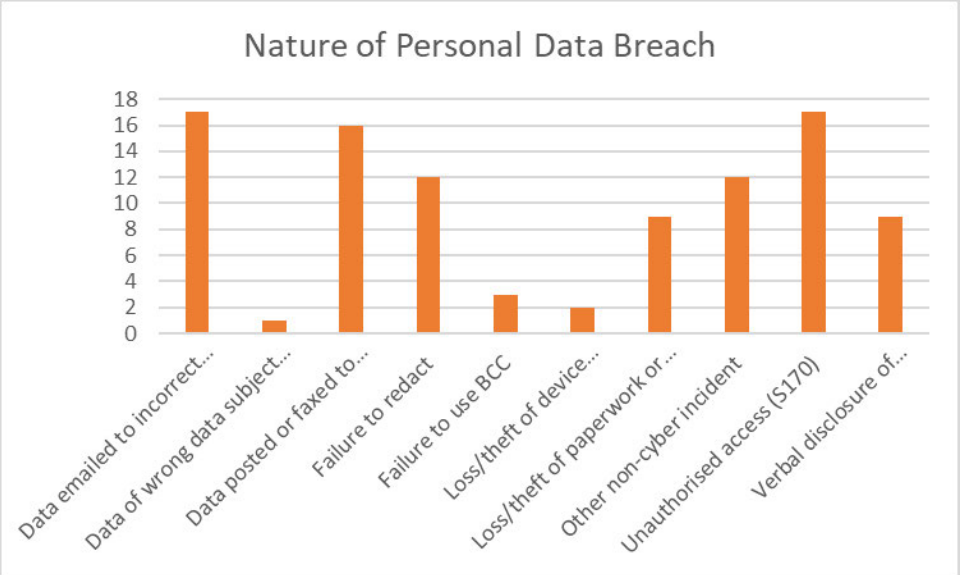
The project team reviewed completed personal data breach reports that were received during three randomly selected weeks in 2022. Using the ICO's definition of vulnerability, we identified cases where the breach affected people at greater risk of harm or where the breach had resulted in people becoming vulnerable. This was a complex and unwieldly task as there is currently no function within the case management system to identify and document cases where people might be at risk of harm. Consequently, almost 560 breach reports received within the determined timeframe were manually reviewed and interrogated, and nearly 18% of the reports reviewed were identified as impacting people in vulnerable situations – which equates to thousands of people impacted. These include situations where sensitive health information was disclosed, birth parents were inadvertently sent location details for their child and as highlighted by the CA report, multiple occasions where a disclosure of information put survivors of domestic abuse at risk. Whilst most breach reports reviewed affected fewer than 10 people, some of the breaches affected hundreds (and in one case, thousands) of people.

A deep dive into 98 relevant breach reports was subsequently carried out, which involved reviewing the breach, understanding how the controller handled the incident and how the breach report was responded to by the ICO. Information from the deep dive was used to populate a Microsoft Forms survey, which informed the analysis (see Annex on page 17 for full report). As identified in the Data Security Incident Trends report (Q2 2022), the project team recognises there are some limitations with the data, for example the information collated is based on reports *received* within the timeframe. Further, some sectors may account for a higher number of breaches involving people who are likely to experience greater harm, for example health, education and local government organisations. However, significant findings have been discovered providing an evidence base for this project's recommendations.

3.2 Statistical findings (see Annex for full report)



The bar graph above shows that the sectors most frequently reporting data breaches within scope were health (26 cases) and local government (25 cases). These two sectors made up over half the total reports affecting people at most risk of harm in the periods analysed.



The bar graph above shows that data emailed or posted to incorrect recipients was a significant concern and totalled almost 34% of the cases reviewed, with unauthorised access representing 17% of the breach reports. The most common category of data disclosed was the person's address.

The breach report asks specific questions of controllers, including whether the incident is likely to result in a high risk to data subjects and whether

those affected had been identified as vulnerable by the controller. Of the 98 breach reports analysed:

- The project team discovered a high risk of harm to people in over 70% of cases, whereas controllers reported there was a high risk of harm in only 40% of the cases reviewed.
- In at least 12% of cases, there was a legal protective factor in place (for example a restraining order, bail conditions, non-molestation order). Out of 12 cases where a legal protective factor was involved, 11 cases involved children and only five cases identified people to be at risk of harm by controllers (all 12 cases were considered at risk of harm by the project team).
- 19 controllers identified the affected parties as vulnerable adults and at least 56 children were impacted by the breaches examined.
- When asked if the breach resulted in a risk to individuals, 31 controllers did not know whether any individuals were at risk.
- Fewer than 6% of cases reviewed were subject to an ICO investigation (civil or criminal).
- In the future there could be opportunity to address issues of vulnerability, risk, harm and impact in closure letters. The data here shows that closure letters could be a powerful route to improve practice and reduce the likelihood of harm in almost 70% of cases.

Personal data breaches have the potential to severely impact those affected, and this was made apparent within the breach reports analysed. One such data breach related to a local authority inadvertently emailing sensitive personal information to a child's birth mother. This unintended disclosure resulted in the birth father threatening to kidnap the child from their adoptive parents. Another incident concerned a system upgrade at a hospital leading to over 15,000 appointment letters having not been sent to patients, causing several patients to miss their medical appointments. These examples highlight how personal data breaches can have a real impact on the lives of those affected and can lead to significant harm.

3.3 Observations

Identifying whether a breach involved a person at risk of harm (or a person who had become vulnerable because of the breach), appeared to be a challenge for controllers who are required to assess the impact of the breaches examined in the breach report form. Similarly, controllers did not routinely assess whether a breach was likely to have resulted in high risk to those affected. Controllers should be best placed to identify risk and harm because of its understanding of its stakeholders and their landscape. Observations identified raise concerns about how controllers interpret sections of the breach report form relating to risk and harm, in

addition to their ability to identify circumstances where people may be particularly vulnerable to their data being unintentionally shared.

Closure letters from the ICO to controllers provided recommendations to avoid reoccurrence of the breach but did not consistently cover increased risk and/ or harm to those affected. Providing clarification and tailored advice enables controllers to understand their obligations and allows for mitigating factors to be implemented where required, thus improving practices in the future and reducing the likelihood of harm. For example:

- Reminding controllers of their obligation to identify and assess the risk to those affected, and effectively respond to harms that may occur because of the breach.
- Providing advice on how to identify, assess and mitigate risk, including suggesting preventative measures which reduce the likelihood of a breach reoccurring.
- Considering additional support that could be offered to those made vulnerable by a data breach, including a reminder that people have the right to lodge a complaint with the ICO.

We recognise that some sectors may account for a higher volume of breach reports due to the nature of the data they process (for example health, education and local government). This provides an opportunity for targeted engagement to be considered regarding identifying and mitigating for issues relating to risk and harm, by understanding what people want from the ICO when they have experienced a significant breach. Targeted engagement could involve the publishing or sharing of guidance in relevant newsletters, sector specific webinars and direct engagement with organisations who provide support to people impacted by a significant breach.

Human error was identified as a factor in 70% of the reports reviewed. However labelling mistakes as 'human error' risks the root cause not being properly investigated. Analysing and addressing root causes will enable controllers to reduce the likelihood of further recurrence and improve harm prevention. Measures to consider include:

- Ensuring all staff have the relevant skills, knowledge, expertise and resources to carry out tasks, and following this up with regular monitoring and verification.
- Having appropriate policies and procedures in place, which are updated and shared regularly.
- Developing a policy which encourages staff to report problems without fear of repercussions.
- Delivering regular briefings to all staff about the importance of highlighting near misses, using case examples if appropriate.

The topic of 'human error' has not been explored in depth and would benefit from additional scrutiny. While we appreciate 'human error' can result in major consequences, it is frequently cited by controllers as a reason for the breach, rather than considering whether the organisation had effective measures in place to prevent a breach from occurring, including rules, procedures, training and technical expertise.

Although not a project objective, we have progressed some of the recommendations highlighted in the Citizen's Advice report, including understanding how serious data breaches occur and identifying solutions to reduce the likelihood of a breach occurring.

Our observations also identified that a significant number of reprimands published in 2022 involved data breaches which impacted victims of domestic abuse, increasing the risk of greater harm for those affected. This trend was highlighted to relevant colleagues and resulted in a campaign calling on organisations to handle personal data properly, to avoid putting domestic abuse victims at risk of greater harm. In addition, this campaign was given internal prominence on Iris, with an article demonstrating our ICO25 commitment to make an impact and help those who need our support and protection.

4.1 How risk and harm should be assessed

Article 33 (1) of the UK General Data Protection Regulation (UK GDPR) requires organisations to report a personal data breach to our office "unless the personal data breach is unlikely to result in a risk to the rights and freedoms" of individuals.

The ICO considers 'risk' as implying a more than remote chance of some harm[2]. When considering the risks to people, organisations should consider the data protection risks that may arise due to the specific processing activity, alongside the impact and/or harms that may be caused. Using the ICO's definition of vulnerability, the project assessed the potential impact of the data breaches researched in the deep dive and identified that 70% of cases demonstrated a high risk of harm, compared to 40% of cases identified by controllers. This exposes a significant disconnect in interpretation of harm that we should be aware of in our communications with controllers, to ensure that harm isn't under-assessed and mitigated against. In the context of personal data breaches, more organisations should be considering the risks that may arise because of the security breach, to identify what data protection harms may be caused to those affected. Further, they should consider the

[2] Further information on the ICO's view of 'risk' can be found in our DPIA guidance: When do we need to do a DPIA? | ICO

likelihood of this manifesting to establish whether the breach meets the reporting threshold.

To improve understanding of harms in a data protection context, the ICO has created a Data Protection Harms Taxonomy[3]. This provides a framework of non-exhaustive examples that organisations could refer to as a starting point, to better identify the data protection harms that may arise from their data processing activities.

One element of this scoping exercise has been to understand the impact of personal data breaches on those who are at greater risk of harm. To develop our own understanding in this area, we used the ICO's Data Protection Harms Taxonomy to map out the potential harms that may arise because of personal data breaches (see Annex 2). These potential harms were not based on our review of the 98 personal data breach reports, as this level of detail was not included in all the reports reviewed. Instead, we undertook an exercise to identify the potential data processing harms that may arise following a security breach using our previous knowledge and experience of working in the Personal Data Breach Service.

Broad examples include:

- **Financial harms:** People who are victims of economic abuse may experience greater financial harms because of a personal data breach, e.g., an adverse impact on their credit rating score may limit a person's borrowing options. Similarly, some people may be at an increased risk of blackmail, exploitation and extortion following a personal data breach. As explained during our engagement with SEA, breaches by financial organisations have led to people being tracked by former abusive partners, with significant consequences.
- **Psychological harms:** People may be at an increased risk of psychological harm due to emotional distress caused following a personal data breach. E.g. The disclosure of HIV status may cause considerable damage and/or distress.[4]

[3] Overview of Data Protection Harms and the ICO Taxonomy

[4] An example of a recent reprimand issues which demonstrates psychological harms being caused following disclosure of HIV status: https://ico.org.uk/media/action-weve-taken/reprimands/4024678/nhs-highland-reprimand-20230314.pdf

4.2 How personal data breaches can impact people

The case review enabled us to identify how organisations assess risk and harm, how they address risk and whether they recognise cases involving people likely to be at greater risk of harm.

We discovered several examples in the research sample of where personal data breaches adversely impacted those at most risk of harm, including the following cases, which were referred to Investigations:

Example 1:

Information supplied by the police [redacted] regarding the data subject was verbally disclosed via telephone to the data subject's ex-partner[5]. [redacted] The information that was disclosed formed part of a live investigation and should not have been communicated to either party. In addition to this, the controller notes within the personal data breach report that [redacted]

The impact of this incident on the affected data subject and their ex-partner was significant. [redacted]

Example 2:

A video of an adopted child and their prospective adoptive mother was accidentally disclosed by a social worker to the birth mother of the child via email.[6] Email addresses of the prospective adoptive mother and father were also disclosed, providing the birth mother with their surname. The birth mother was not entitled to receive this information.

Concerns were subsequently raised by the prospective adoptive parents [redacted]

A court order had been in place preventing the names and addresses of the adoptive parents from being disclosed and their identification potentially undermined the adoption process.

[5] Case reference: [redacted] (Case management system: ICE360)

[6] Case Reference: [redacted] (Case management system: ICE360)

These incidents demonstrate that the impact of personal data breaches on those affected can be significant. This applies to cases where a person has become at increased risk of harm because of a personal data breach (the data subject and their ex-partner cited in Example 1, and the prospective adoptive parents in Example 2), and cases where people are already considered to be vulnerable (the adopted child in Example 2).

Our case reviews also considered what type of detriment was being reported by controllers within their personal data breach reports. The two most common harms cited include:

- Psychological harms (emotional distress, anxiety, fear, embarrassment), and
- Loss of control of personal data.

Whilst these were the harms reported most frequently, it is important to also consider that harms will be weighted differently depending on the context of the personal data breach, the likelihood and severity of the risk, and the action taken to mitigate the risk. For example, an additional harm that was reported less frequently was bodily harm. However, the severity of this harm has the potential to be significant, particularly for those who might need additional support to protect themselves. Another factor to consider is that the risk of harm being caused to those affected can often be mitigated or aggravated when compliance with other data protection principles is considered. Failure to comply with the accuracy principle may increase the likelihood of detriment being caused. For example, disclosure of a person's location because an address has not been updated on a system, leading to information being shared with the wrong person.

4.3 How organisations are assessing risk and harm

In relation to how controllers are assessing risk, Article 33 (3) of the UK GDPR requires organisations to describe the likely consequences of the personal data breach. As previously mentioned, the ICO's personal data breach report form asks the controller to confirm whether the breach is likely to result in a high risk to the affected data subjects. As referenced in the findings section above, we identified that controllers do not appear to be assessing the likelihood of risk adequately.

This is demonstrated in the responses to the question on whether the breach is likely to result in a high risk to data subjects, where 31 controllers selected 'not yet known' as their response – suggesting that controllers do not have a good understanding of how to identify and assess risk. This is further evidenced in Example 1 cited above, where the

controller also selected 'not yet known' to this question - despite acknowledging that the distress caused [redacted]. Providing controllers with the tools required to conduct adequate risk assessments - including relatable examples – enables improved outcomes for those affected by a data breach.

Regarding how the ICO responds to personal data breach reports, the decision letters sent to controllers frequently reference the need to address the impact of data breaches on people. However, our case review demonstrates the need to provide further tailored advice to controllers on identifying and addressing risk and harm in multiple cases. This will be discussed further within our recommendations.

5.1 Recommendations

In determining our recommendations, the project team has identified opportunities to improve how the ICO responds to issues of vulnerability in personal data breach reports. Implementing practical technical changes to our case management procedures, including ICE 360, would enable those at greater risk of harm to be more easily identified and tracked, allowing us to monitor, measure and analyse trends and take informed steps to address them. Delivering targeted engagement using resources relating to risk and harm in data protection would offer additional support to controllers. For example, this could support controllers in identifying security and procedural measures appropriate to the type of personal data they are processing. This would allow them to take a more informed, thorough approach to safeguarding the personal data of those who are at greater risk of harm. Developing existing internal guidance in the form of Knowledge packs, delivering relatable 'outside in' events, sharing resources and good practice across the office would encourage an effective identification of, and response to, issues relating to risk and harm. This would enable us to widen the scope of the people we can empower through our guidance and decision making, particularly those who have no choice but to share their information in order to access services and support.

Our recommendations are addressed in the table below and are presented to consider what the issue is/ what did we notice ('What'), why is this important/how this has/ might impact people ('So what'), and what we can do to reduce negative impact/ improve the situation (Now what)[7]:

[7] Relating to an Agile framework and explained here Liberating Structures - 9. What, So What, Now What? W³

1. Identifying, recording and monitoring cases involving people at risk of harm		
What?	**So what?**	**Now what?**
Controllers do not consistently acknowledge vulnerability when reporting a personal data breach. For example, of the 77 cases which did **not** identify a vulnerable adult, the detriment recorded included emotional distress, bodily harm and discrimination.	Issues of risk and harm are not effectively acknowledged and/ or addressed. Controllers' perceptions and understandings of the term 'vulnerable' may not be consistent and they may not understand how this question has been framed. Therefore, controllers aren't making the connection between harm caused by the breach, resulting in people being at increased risk.	A potential solution for the ICO could be to explain to controllers how it interprets vulnerability, risk and harms and consider how relevant questions are framed, both on the breach report form and when controllers contact us directly to report a breach. For example, by asking the controller 'Does this breach impact the personal data of a person likely to be at risk of harm' with a required response of Yes/ No/ Not known. This would have the potential to reduce the impact of a data breach on those affected, particularly those at greater risk of harm[8]. This recommendation could be considered by the PDB Service, supported by the Communities Working Group.
Language used to describe people likely to be at risk of harm has changed.	We need a consistent cross-office approach and shared understanding of risk and harm and how this might apply to people who might be in situations where they are at risk.	Ensure that all staff understand the approach to be used when talking or writing about people who might be at greater risk of harm – including an understanding that this may be a temporary phase as a direct result of a data breach. For example, where victims of domestic abuse have again been

[8] John Edwards, Information Commissioner, delivers a keynote speech at IAPP Data Protection Intensive UK. | ICO

		required to move home/ job/ school because of a disclosure of their location. This recommendation could be considered by the Communities Working Group.
Case management systems do not include a function to effectively record, track and monitor cases which involve people at risk of harm.	Research is time-consuming, data security trends regarding risk and harm are difficult to analyse, links between a data breach from a controller and a complaint received from an affected person are not always apparent, and identifying organisations that repeatedly breach personal data rights of people at higher risk of harm are not monitored.	Implement processes and systems which allow the ICO to proactively identify and monitor issues of vulnerability, demonstrate our interactions with people at most risk of harm, support outcomes relating to inclusivity, measure the impact of ICO25 objectives, effectively link associated cases, identify organisations who may require additional scrutiny, and add value to data security incident reports. This recommendation could be considered by the PACE 5 team[9] and discussed with colleagues working on the Enterprise Data Strategy, to determine how we can support interoperability between current systems and processes, to enable instances of harm to be identified and monitored[10]. This recommendation would have benefits for colleagues across the office including PDB Service, PADPCS, Research and Economic Analysis.

[9] PACE 5 team is working on a project looking at customer service for individuals who may be vulnerable.

[10] Knowledge - How-Can-We-Help-You-Full-Report-1.pdf - All Documents (sharepoint.com)

Less than 6% of cases reviewed were considered for further investigation (either civil or criminal).	A limited number of referrals could result in more serious cases being missed. Additional scrutiny allows for further regulatory interventions to be considered, enabling detriment to those affected by the breach to be discovered.	Review internal processes to determine the most effective way for cases to be referred and considered for additional internal scrutiny, which could result in improved outcomes for those affected by the breach. This recommendation could be considered by the Communities Working Group, supported by PDB Services and Investigations.
2. Increasing acknowledgement of harm in our communications with customers		
Communications with controllers reporting data breaches should acknowledge risk and harm, particularly where a vulnerable situation has been identified.	Closure letters are a powerful tool and could enable improved practice, reducing the likelihood of recurrence. Ensuring that risk, harm and potential harm are identified/ acknowledged in communications with controllers provides the ICO with opportunities to advise on steps to consider when identifying risk and mitigating harms.	Review internal processes to enable controllers identify risk and harms caused by a breach effectively, so that mitigating steps can be implemented. This might include the controller offering appropriate support to those affected, particularly where they have experienced physical, psychological, or financial harms. Consider reminding the controller of their obligations regarding Article 13(2)(d) UK GDPR, which require the data subject to be informed (at the time that personal data is obtained) of the right to lodge a complaint with the Commissioner. This could increase the number of connected cases received by

		PADPCS, which provides additional insight to internal investigations into a breach. This recommendation could be considered by the PACE team, supported by the Communities Working Group, PDB Service and PADPCS.
3. Acknowledging risk, harm and situations which increase vulnerability in our guidance		
Controllers do not consistently identify and assess risk and subsequently mitigate any harms resulting from a breach.	Appropriate safeguards are not identified and implemented by controllers, leading to risk of greater harm for those affected by the breach. Consider how this aligns with ICO25 principles, including empowering people to confidently share their information to use products and services.	Review existing guidance and information to determine how effective this is in enabling controllers to identify and assess risk and harm, particularly for those people who may need additional support[11]. Acknowledge that the absence of 'high risk' does not mean that the impact of a breach is 'low risk', and that a breach can often have long-term implications for those affected. This recommendation could be considered by the PACE team and the Communities Working Group.
Information about assessing risk and harm is not centrally stored.	Controllers may find it difficult to understand their responsibilities regarding identifying risk, considering	Consider the development of a risk/ harms hub, where tailored and targeted advice and information is available for both controllers

[11] Understanding and assessing risk in personal data breaches | ICO

	vulnerabilities and mitigating harms. This can result in safeguards not being considered or effective following a breach, limited information being provided to the ICO about the breach and cases being closed without additional scrutiny. Providing effective support to controllers enables the ICO to promote greater data protection for people who are disadvantaged because of issues relating to information or power imbalances.	and those affected by a breach. This would provide an additional framework for controllers to identify, acknowledge and incorporate issues regarding risk and harm into their data protection practices, policies and procedures. The 'hub' could include: - Relatable case studies highlighting the risks of personal data not being processed securely and enabling controllers to identify ways to improve their practices. - Examples of good practice regarding processing of data of those at greatest risk of harm. - Guides and FAQ's for SME's, particularly those likely to process data of people at greater risk of harm. - Additional guidance and information regarding assessing risk in the context of vulnerability and data protection harms. - Advice for controllers to analyse root causes of a breach and reduce the likelihood of recurrence. - Consistent information for those affected by a breach, to enable an effective journey towards a complaint. This recommendation could be considered by the Communities Working Group.

4. Staff initiatives		
Inconsistencies can occur when considering risk, harm, recognising vulnerabilities and understanding next steps.	Research by the UK Regulators Network alongside Britain Thinks[12] suggests that encouraging frontline staff to be proactive in recognising vulnerabilities when they interact with customers could be integral to supporting those in vulnerable circumstances. This benefits controllers and would also be beneficial for the ICO. Proactively recognising vulnerability has been trialled within the 2V Network delivered by PADPCS. This demonstrates how an empathy-led approach and focused training can improve responses made to customers in vulnerable circumstances. Having a greater alignment across office enables a consistent approach to be implemented.	Promote a consistent approach to risk, harm and recognising situations which could create vulnerabilities. Further develop an empathy-led approach to how we interact with customers, including the use of active questioning and understanding the links between vulnerabilities and harm. Ensure appropriate resources are available to staff to provide opportunities to empower and inform people who are at most risk of harm. Embedding principles of psychological safety enables initiatives discussed to be most effective. This recommendation could be considered by the Communities Working Group.

[12] UKRN/ Britain Thinks Literature Review on Identifying Vulnerable Consumers | UKRN: the UK Regulators Network

6.1 Next Steps

In delivering next steps, this report is being published on Iris and is being shared with teams who have worked with us on the project, and/ or who have a specific interest, including PDB Service, PADPCS, Investigations, SME Service, Research and Insight and the Head of Communities. We've collaborated with all these departments throughout the project and have been grateful for their support. This will enable the recommendations to be considered and relevant actions determined to ensure we deliver a coordinated response to issues of risk, harm, and vulnerability. What's happening already is a new PACE team is being developed, to look at customer services for people who may be in situations where they are at risk. The PACE team will use this report as part of its evidential basis. Further, the report will be presented at the first Communities Working Group meeting where there will be a discussion about the recommendations and actions that sit outside the scope of the PACE project.

The learning from this project will be used to follow up on the ICO25 commitment to safeguard the most vulnerable, by using targeted engagement with controllers to enable them to improve their compliance, and by empowering people should they experience a breach. This work will require continued collaboration with colleagues, particularly those from the PDB Service, so that the wealth of knowledge and experience from this department is utilised.

7.1 Conclusion

The motivation for this project came from identifying that a significant number of data breaches involved people who were at greater risk of harm because of the breach. To put this into context, whilst for many people, having a letter sent to the wrong person may at most be inconvenient, for some people, we have seen how this can be catastrophic. In considering the people who were most likely to be impacted by a breach, the project challenges the ICO to consider whether it can do more to prevent harm being caused.

Carrying out the deep dive of 98 breaches has provided a unique opportunity to scrutinise the reports and gain significant insight into the complex nature of data breaches, and how the ICO responds to them.

Throughout the life of this project there has been increased awareness across the office about the impact of a personal data breach. PDB Service continue to provide support and guidance to organisations that experience data breaches and are often the first to identify high profile incidents that

may generate media attention and/ or require immediate prioritisation. PADPCS have demonstrated how they can 'do things differently' using 2V Network practices by publishing an advent calendar in December 2023, sharing insights into the impact they have had on customers. At least two PACE teams have shown an interest in how inappropriate data sharing can impact people and significantly, a PACE team has been stood up to consider the response we provide to people who may be in vulnerable situations, and who have experienced a data breach.

Our discovery throughout the project has highlighted that even those organisations whose primary role is to safeguard people (including law enforcement, health and social care) have breached personal data with sometimes catastrophic results.

In concluding this project, it is clear that our recommendations address ICO25 priorities regarding safeguarding and empowering people (particularly vulnerable groups), producing relevant 'off the shelf' products and providing assured regulatory advice. The project closes at an exciting time for the ICO, where colleagues are working on a number of synergetic activities, including the Enterprise Data Strategy and the Regulatory Action Framework, which will contribute to harms being identified, monitored and effectively responded to, in order to reduce harms experienced by those at greatest risk. The topic of vulnerability is a multi-faceted one which regulators including the ICO are making a priority, most recently via the Vulnerability Working Group and will be continued through the refreshed 'Communities Working Group' and the new PACE team. In supporting cross-office activity to deliver the recommendations, we will further develop the impressive body of work delivered by our colleagues in the PDB Service.

Annex One:

Personal Data Breaches – The harms and impact on vulnerable individuals (MS Forms document detailing research carried out).

Annex Two: Harms Taxonomy (see below):

Annex Two

The ICO's Data Protection Harms Taxonomy

The **Personal Data Breaches – harms and impact on vulnerable individuals** project group has provided some initial views of harms and potential harms below, based on our research including a deep-dive of 98 breach reports received by the ICO.

The taxonomy will be iterative and updated as more information is available to us. The project team has engaged with organisations supporting those who may be impacted upon.

Type	Category	Description	Potential manifestation of harms
Individual	Financial harm	Negligently, knowingly, or purposefully paving the way for financial losses to occur	• Victims of economic abuse can experience long-term impact, which may be compounded following a breach. For example, having to again move home/ job/ school, impact on credit rating, fraud. Financial harms likely to be greater for those who are already vulnerable. • Information revealed might be sensitive used to blackmail or threaten an individual or enable a former abuser to exploit finances again. • Individual may experience severe emotional distress and be unable or discouraged from working following a breach, particularly where there have been threats made, location identified, sensitive data revealed. • Cyber incidents designed to extort data for financial gain. Vulnerable person may be especially susceptible.
	Bodily harm	Negligently, knowingly, or purposefully paving the way for physical injury to occur	• Tracking vulnerable individual following breach of location, leading to physical and psychological harm, emotional distress, suicide or other self-harm. • Risk of/ fear of abduction of children.

	Costs of avoiding/mitigating harm	The cost in terms of time or money incurred in the avoidance or mitigation of harms or vulnerabilities related to data privacy	• Target hardening/ security costs already in place which may need to be changed, legal costs incurred re preventative measures ie NMO, name changes, legal processes involved with acquiring a new identity. • Changes to IT systems/ policies where breaches have resulted in data being shared extensively, e.g., in education/ workplace settings. • Emotional cost to vulnerable individuals whose data has been breached.
	Discrimination	Harms arising from discrimination or bias (either conscious or unconscious)	• Sensitive information more publicly available including SEND, medical information, protected characteristics, fostering/ adoption details. May result in individuals being subject to bias/ discrimination in school/ work etc. For example, HIV status revealed, adoption information shared without consent.
	Unwarranted intrusion	Unwanted communications or intrusions that disturb tranquillity, interrupt activities, sap time or increase the risk of other harms occurring	• Unwanted contact leading to harassment and stalking behaviour. For example, s170 breaches, where member of staff accesses information without a business need, to identify details of an individual. Impact on those who are vulnerable likely to be significant. • Needing to have surveillance at home/ work/ school where this was not previously required. • Isolation due to concerns about being out in public.
	Loss of control of personal data	Harms from thwarted expectations, through misuse, repurposing, unwanted retention or continued use	• Inability to manage risk associated with data being in public domain and not known who might have access to this. Unknown who data may have been

		and sharing of personal data, including a lack of commitment to the accuracy of data or lack of transparency	shared with, information available on social media and difficulties getting this removed. Impact this loss of control may have on mental health and well-being, in addition to renewed trauma. • Physical/ emotional harm experienced as a result of breach. For example, s170 case where individual accessed patient records and discussed sensitive information in child arrangements hearing, leading to negative outcome for both DS and their children. • Not having access to vital data, for example unique records which may have been lost in the post regarding adoption/ fostering cases. Impact on all parties including birth parents. • Time and emotional energy to establish what data might have been lost/ become unavailable and how to retrieve data. Impact greater where individuals are vulnerable. • Limited awareness of dp rights – individual may not know how to exercise their rights or seek redress should their data be compromised.
	Lack of autonomy; manipulation and influence	Restriction, coercion, or manipulation of people's choices or their ability to make an informed choice	• Individual experiencing re-traumatisation, particularly where the breach has happened sometime after lives are more settled. • Isolation, fear about going out unaccompanied. • Having to restrict daily routines due to not knowing what has happened to personal data/ unsure what the impact might be when data has been shared inadvertently. For example, HIV status shared as a result of a breach. • Coercive control may increase.

			• Individual may have increased feelings of doubt and fear with organisation and how their data has been handled. Restriction in making informed choices, may choose not to further engage with organisation and other support services.
	Psychological Harms	Negligently, knowingly, or purposefully paving the way for emotional distress or disturbance (embarrassment, anxiety, fear) to occur	• Existing trauma exacerbated as a result of breach. Affects mental health of all concerned including any children and also impact on current and future relationships with friends, family, school, work etc. • Having to re-explain situation to an additional group of people, for example having to share details of trauma, abuse, HIV status, adoption, additional needs etc. Impact includes embarrassment, low self-esteem, re-living trauma, poor mental health, substance misuse, self-harm etc. • Revisiting counselling/ taking medication. • Psychological impact affecting physical health and well-being. • Impact on those who are/ have been vulnerable more significant, for example victim of domestic abuse whose location has been breached is at greater risk of psychological harm. • Can lead to physical harm.
	Chilling effects	Reduced use of services or activities due to an actual or perceived risk of potential harm. And hence, a reduction in the benefits that may have been achieved.	• Reluctance to further report issues because let down by systems that should have protected, reluctance to use support services as documented by Citizens Advice. • Victim of bullying and harassment, for example child who has experienced a breach of SCD may become more withdrawn, increase self-harm etc.

			• Isolation, avoiding social interactions and relationships which might benefit. • Impact of any financial issues ie credit rating reduced. • Lack of trust, reluctance to report other crimes to police/ provide data to social care/ legal services etc due to actual or perceived risk. • Restricted movement and increased isolation may result in further abuse – for example, research suggests women who experience domestic abuse are targeted in the same way as an abuser would target a child victim of abuse.
	Adverse effects on rights and freedoms	Negative impacts on rights and freedoms in and of themselves	• May not be aware of data protection rights and therefore not know how to exercise them. • In situations where data has been lost, individual may not be able to make a SAR. For example, where a child has been fostered/ adopted and their data cannot be located, this may have a more significant impact particularly where this involves information about their origins, family life, medical history etc. • Impact on physical and psychological well-being.
Societal	Damage to law and justice	Restrictions on or subversion of legislative intent, or legal or judicial process	• Reputational damage to law and justice can result in wide-scale chilling effect – not just on victims and witnesses but on wider community. For example, breaches where records relating to child sexual abuse have been inadvertently shared may result in other victims not coming forward. • Risk of increased hate crime where personal data relating to HIV status, transgender status, additional needs etc has been disclosed.

	Damage to media, democracy, information and public discourse	Negative impacts on media, democracy information and public discourse at a societal level	• Mistrust leading to chilling effects on freedom of expression. • Individuals not registering to vote as they are concerned that this information is made publicly available (ability to have this information removed has several barriers). • Recent requirements for individuals to have photographic ID in order to vote at polling stations. People who are considered vulnerable may not have access to photographic ID and the process to achieve this can be complex. • People who are vulnerable may be more easily coerced to vote in a particular way. • Difficult to become engaged in public debate when you have little resilience, time and energy is spent on managing your vulnerabilities.
	Damage to public health	Harms resulting in adverse health outcomes for society	• Mistrust of how your health data is managed following a breach, particularly where unauthorised access to medical records has occurred. • Impact of a cyber incident on medical establishment, including loss or lack of availability of data, inaccuracies, patients not receiving appropriate care and support, serious ill-health and death. • Impact of a breach can lead to increased need for psychological and physical support resources.
	Damage to the economy	Negative impacts on the economy that are significant at the local,	• Individual cases may not have a great impact but research in 2014 identified the cost of domestic abuse in England and Wales to be £23 billion pa.

		regional, or national level, or for a specific sector	• Loss of trust from potential adoptive parents, leading to more children remaining in care at a significant cost to the public purse. • Increased vulnerabilities resulting in fewer people contributing to the economy. • Organisations diverting resources from regular tasks due to resolving/ managing breaches that have been made.
	Damage to the environment	Negative impacts on the environment either directly or indirectly resulting from misuse of data or mitigation of associated risk.	• N/A at the moment

Harms Taxonomy as of 3 August 2023.