# Model Action Plan for Responding to Significant Data Breaches

## Introduction

1. The Model Action Plan (MAP) is designed to provide a consistent, coordinated and robust approach for all government departments and arms-length bodies (hereafter collectively referred to as 'organisations') to respond to significant personal data breaches. Its foremost concern is to ensure the wellbeing of those affected by a significant breach, including their personal safety, privacy, and legal rights regarding their data. The Model Action Plan introduces mandatory central reporting of significant data breaches to enable the government to analyse the nature, scale and trends of incidents, and to identify systemic weaknesses, which can then be shared across government for effective mitigations.

2. **A significant 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 transmitted, stored or otherwise processed that:

    a. potentially affects a large number of data subjects by exposing them to the risk of serious harm, or a smaller number of data subjects who have a higher profile (e.g. high profile public figures, public sector staff in sensitive roles, people in witness protection schemes), or

    b. poses significant national security risks outside of the impacts highlighted above, e.g. significantly exposing the UK to espionage or affects the proper operation of critical national infrastructure, or

    c. affects multiple organisations, including incidents originating from third-party suppliers and subcontractors, or

    d. is likely to cause significant financial harms, threat to life, critical system loss, lead to significant media/parliamentary interest (e.g. due to its sensitivity), or the exceptional exposure to risk that certain individuals possess (e.g. Cabinet Ministers).

3. **All significant personal data breaches that meet the statutory threshold for reporting to the Information Commissioner would be expected to meet the criteria above.**

4. Given the sensitivity of some of the personal data processed by HMG, significant personal data breaches can cause physical harm, financial loss, emotional distress, reputational damage and a wide range of other negative effects. They can also have wide-ranging consequences for organisations, e.g. fines, reputational damage and risk for the UK as a whole, e.g. damage to national security.

## Purpose

5. The purpose of this MAP is to:

    a. provide a clear process for how best to respond to significant personal data breaches,

    b. facilitate coordinated responses to significant breaches affecting multiple organisations,

    c. outline the requirements and process for escalating incidents to the Accounting Officer, the GSG incident response team (within the Cabinet Office) and the Government Chief Data Officer and the Government Data Protection team (Government Digital Services, Department for Science, Innovation and Technology).

    d. facilitate a prompt return to business as usual following breaches,

    e. helps organisations meet their legal obligations set out in UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025,

    f. support collation of cross government insights at the centre of government to address systemic weaknesses,

    g. improve accountability and transparency to build public trust in government's ability to recover following significant personal data breaches and

    h. learn lessons to make effective improvements to avoid recurrence of such breaches.

6. This MAP has been informed by expertise and best practice from the Information Commissioner's Office (ICO), and should also be read in conjunction with 'Principles for securing personal data in government services' on gov.uk, particularly Principle 1 - i.e. **Plan your response to personal data breaches before they occur**

## Audience

7. This MAP is intended in particular for colleagues involved with identifying, managing and responding to breaches across government, such as data protection officers (DPOs) and security teams. The MAP can be used as an effective tool for senior leaders in ensuring their organisation has adequate and effective significant personal data breach response plans in place and for those senior leaders who may be required to oversee or manage a significant breach.

## Applicability

8. Cyber security breaches are coordinated by the Government Cyber Coordination Centre (GC3). However, if the cyber security breach impacts wider government security outside of the cyber realm, GSG incident response may coordinate the response to that impact.

9. If the breach involves personal data and meets the significant personal data breach definition in point 2 above, the organisation's DPO retains their statutory role and will still report the breach to the ICO on the organisation's behalf within 72 hours in line with the guidance and process outlined on the ICO website. Likewise, even if the breach does not yet appear to have involved personal data, it may facilitate the theft or publication of such data in future. As such the principles set out in this MAP remain relevant.

10. **This MAP does not replace local departmental policies.** Organisations should review their local departmental policies to ensure they're aligned with the MAP. Incidents should be categorised and managed in accordance with your organisation's crisis management policy.

11. Departmental action plans should be simulated periodically (in most organisations this should be annually) against a hypothetical significant personal data breach, e.g. through a tabletop exercise, to ensure decision-making timelines are realistic and that the organisation is able to meet the 72-hour reporting requirement.

12. This MAP is not a substitute for data protection and/or legal advice. In the event of an actual or suspected breach, organisations should contact their respective data protection officers and lawyers, as appropriate.

13. All Departments are expected to have arrangements in place to be able to sustain a crisis/incident response, protecting the welfare of the staff involved in the response, as directed by the Cabinet Office "Amber Book" (UK Government Crisis Response Framework – UKGCRF), which is the core crisis response framework that sets out roles, responsibilities, structures and how decisions are made through the lifecycle of a crisis. Although the Amber Book does not deal with individual data breaches, it would become relevant if a significant data breach escalates to a wider crisis (e.g. national security impact, disruption to essential public services, system-wide failure, large-scale harm or reputational crisis requiring central coordination).

14. All incidents which are reported to the ICO must also be reported to DSIT and GSG. **The information included in the ICO report must be used to escalate the incident centrally to avoid duplication of effort.**

15. Government departments must report cyber incidents to the NCSC when they are aware of an incident that could impact a UK essential service or national security (see paragraph 24 below).

# Model Action Plan

## Phase 0 - before any breach occurs - preparation

1. **The organisation as data controller is responsible for the protection of personal data they process** and should prepare for significant personal data breaches before they occur as part of its usual assurance process.

2. This should include:

    a. An organisational plan and processes for how to identify personal data breaches, e.g. ensuring that data processing is set up to facilitate detection of breaches.

    b. Confirmation that any data processors are contractually bound to assist in the identification of and response to breaches, as per UK GDPR Article 28. This should include strict service level agreements (SLAs) mandating that third-party suppliers/contractors must notify the department within 12 to 24 hours of discovering a suspected personal data breach.

    c. Complete and up-to-date register of information assets, including critical assets.

    d. An organisational plan and processes for how your staff should handle the breach itself and mitigate its immediate impact (including in an out of hours scenario).

    e. Clearly defined roles and responsibilities for the SA, DPO, and other senior staff with regards to breaches, particularly in terms of reporting and safeguarding individuals from potential harm.

    f. Identify and record cyber points of contact in organisational response plan.

    g. Clear plan outlining how your organisation will communicate internally if systems are down, approved alternative channels, how staff get updates, how communication with partner organisations, suppliers and service users are maintained.

    h. Include clearly defined roles and responsibilities for CISOs and cyber teams in relation to data breach arising from a cyber incident

    i. Clearly defined routes and thresholds for escalation.

    j. A clearly defined process for reporting significant personal data breaches to the relevant authorities, including roles responsible for reporting and to ensure this occurs within the statutory timeframes.

    k. Publication, training and testing of these processes within your organisation.

l. The creation of pre-drafted, pre-approved communication templates for common accidental breach scenarios (e.g., misdirected emails, lost devices and hidden data).

m. The establishment of a lessons learned process to review incidents and avoid reoccurrence, with the power to drive necessary reforms.

## Phase 1 - within 24 hours of identifying a significant breach - initial steps

**Confirm and escalate the personal data breach**

3. Staff must immediately inform the relevant internal staff in the event of a significant breach, as directed by local policies and processes. Typically, this will include some combination of line managers, SAs, and DPOs.

4. Organisations must ensure that staff are aware of the correct local procedure(s), including:

    a. Who they need to inform.

    b. How to do so, e.g. including contact details, out-of-hours helplines, etc.

    c. What information they need to include while doing so.

5. This information must be proactively communicated to staff, but also easily accessible in the event they need to look it up (e.g. via intranets).

6. In the event that organisations face multiple personal data breaches simultaneously, they must be ready and able to triage to identify the most critical aspects quickly and effectively.

**Containment of a personal data breach**

7. Once informed of the personal data breach, the organisation must seek to immediately contain the breach, via a mix of:

    a. **Technical & Cyber action:** e.g. isolate affected systems, remove published content, lock-down folders, disable compromised accounts, block external threat, recall sent documents, ask for immediate and thorough deletion, revoke access privileges, identify the source, preserve evidence, document decisions.

    b. **Physical action:** e.g. disable key cards, search for and recover lost objects/materials, ask for immediate destruction.

    **c. Legal advice:** if appropriate, notify and seek legal advice from the organisation's lawyers, including whether additional steps can or should be taken to limit the impact of the breach. This should be done in parallel to steps (a) and (b) above, unless there is a concern that action would fall foul of

other legal obligations. Where this is the case, escalate as needed for urgent advice.

8. In some circumstances, if a data subject is facing an imminent safeguarding concern, the organisation should inform the police, at the earliest opportunity and seek to mitigate the threat through containment of the breach. For example, due to the release of information relating to the protection of vulnerable children; individuals in witness protection; or those being shielded from domestic violence.

9. In all cases, consider whether services can continue, whether they require short-term modifications, or if they need to be suspended altogether.

10. If personal data is being processed on the organisation's behalf by a third party supplier (e.g. a contracted service provider), the organisation must assess if personal data remains at risk, and if so, consider whether immediately ceasing the flow of additional personal data is appropriate, e.g. to prevent further breaches from occurring. Exceptions may apply if doing so would create greater harm and/or undermine the response (e.g. in informing affected data subjects).

## Phase 2 - as soon as possible - assessment of risk and severity (but not later than 48 hours)

**Assess the severity of harmful effects**

11. The organisation must assess the severity of the breach, in particular to the data subjects. You must assess the "risk to rights and freedoms", that is, any negative consequences that could follow from the breach such as safeguarding issues, identity theft or significant distress.

12. Each breach will need to be assessed on a case by case basis and there is no one size fits all methodology for risk assessing data breaches. The harms organisations encounter will differ based on their localised context and types of data being processed.

    Additional information to help inform consideration of impacts is available from the ICO here.

13. It may not always be clear if a personal data breach has occurred. In cases where a breach is only suspected, the data controller is unlikely to be "aware" of the breach in the terms of their UK GDPR responsibilities until the facts can be established. A precautionary approach should be adopted, and if a breach having occurred is more likely than not, then data controllers must consider commencing with risk assessment and notification steps.

**Ascertain if the personal data breach is 'significant':**

14. A 'significant' 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 transmitted, stored or otherwise processed that:

a. potentially affects a large number of data subjects by exposing them to the risk of serious harm, or a smaller number of data subjects who have a higher profile (e.g. high profile public figures, public sector staff in sensitive roles, people in witness protection schemes), or

b. poses significant national security risks outside of the impacts highlighted above, e.g. significantly exposing the UK to espionage or affects the proper operation of critical national infrastructure, or

c. affects multiple organisations, including incidents originating from third-party suppliers and subcontractors, or

d. is likely to cause significant financial harms, threat to life, critical system loss, lead to significant media and parliamentary interest (e.g. due to its sensitivity), or the exceptional exposure to risk that certain individuals possess (e.g. Cabinet Ministers),

15. All significant personal data breaches would be expected to meet the statutory threshold for reporting to the Information Commissioner.

16. If the breach is classed as 'significant', the organisation must immediately activate its crisis incident response plan and appoint an incident manager (this should be an SCS1 or above based on the incident's severity). Some organisations will have in place Bronze, Silver and Gold command structures.

17. The incident manager should set up a communication channel for all key organisational stakeholders involved in dealing with the breach. The incident manager should maintain a rhythm of regular updates. The DPO maintains their statutory role. Depending on the nature of the incident, data protection, information security, cyber security, and knowledge and information management expertise must be involved in the containment and investigation following an incident.

## Phase 3 - within 72 Hours - notification, ICO reporting and escalation

**ICO reporting**

18. When an incident is assessed to have crossed the statutory threshold for reporting to the ICO, this must be done within 72 hours of your organisation learning of the breach. Typically, this would be done by the DPO, availability permitting. **If you miss the 72-hour window, you must provide a clear reason for the delay.**

19. Contact with the ICO must be done in the first instance via this web form. (https://ico.org.uk/for-organisations/report-a-breach/). Organisations will be asked to outline the following information:

    a. Nature of the breach (i.e. what happened).

    b. Categories and approximate number of data subjects/records.

c. Estimated impacts and their likelihood.

d. Measures taken or proposed to mitigate the impacts.

20. In the event that an organisation has completely lost access to the internet, they can contact the ICO via phone on: 0303 123 1113. This is not the preferred route for reporting or notifications.

21. In the event of a complex breach where not all information can be provided within the timeframe, you can report in instalments; i.e. your initial report must be submitted within 72 hours, but information gaps can be filled over time. **It is better to send an incomplete report on time than a full report late (this should be accompanied by an explanation of what is missing, why and when it will be provided).**

22. When a significant personal data breach involves more than one organisation, the reporting process depends on the role each organisation plays in relation to the personal data. Where more than one independent controller is involved (but they are not joint controllers), the expectation is that each controller needs to assess the breach independently and decide whether it needs to report. More than one notification to the ICO may therefore be appropriate. Where organisations are joint controllers, they may submit a single breach notification to the ICO, by agreement. Joint controllers must ensure roles and reporting responsibilities are clearly documented and operationalised. It is particularly important to involve the Government Data Protection team within the Office of the Government Chief Data Officer in DSIT to support coordination.

**Reporting and escalating a significant personal data breach within Government**

23. You must notify significant breaches (and particularly those impacting national security or across multiple organisations) within the 72-hour window to:

    a. Your organisation's Accounting Officer (typically a Permanent Secretary or equivalent).

    b. The Incident Response team within the Government Security Group (GSG) in the Cabinet Office:
        - Email: gsg.response@cabinetoffice.gov.uk

    c. The Government Data Protection team within the Office of the Government Chief Data Officer in DSIT.
        - Email: CentralGovDataProtection@dsit.gov.uk

24. For cyber-related incidents only, [23.b] must be replaced with:

    a. GC3 and the National Cyber Security Centre (NCSC)
        - NCSC Reporting Portal at https://report.ncsc.gov.uk/

25. All incidents which are reported to the ICO must be reported to DSIT and GSG. **The information included in the ICO report should be used to escalate the incident centrally to avoid duplication of effort.**

26. The requirement to contact DSIT's Government Data Protection team was introduced in April 2026 as a mechanism to ensure that significant breaches can be formally logged. This data will be collated and analysed, and form part of the Government's publicly available annual assurance statement on data protection.

27. Organisations are strongly recommended to use a copy of the same web form submitted to the ICO when contacting DSIT, Cabinet Office and others, to avoid duplication of effort. You must also provide an ongoing point of contact (ideally your DPO).

**Informing data subjects**

28. Personal data breaches can have catastrophic consequences for individuals: for their privacy, their wellbeing, and even their safety. It is vital that our response is both attentive to their physical needs and also compassionate to the distress they may feel. **Please bear this in mind throughout.**

29. If the breach poses a high risk to data subjects, then by virtue of Article 34(1) UK GDPR organisations must notify the data subjects directly that their personal data has been breached, unless doing so would cause more harm. If providing direct notification would involve disproportionate effort, then it may be possible to issue a public communication to draw attention to the incident instead.

30. There may be occasions when you do not have a legal obligation to notify data subjects, but it is nevertheless something you decide to do as a matter of good practice.

31. When communicating with data subjects, you should seek to provide clear information, actionable advice, and be helpful in what they can and/or should do next. Proactive communication can lessen reputational damage and can help prevent subsequent threats (e.g. phishing campaigns) becoming successful.

32. Due consideration should be given on which communications channel is the most appropriate for notifying the affected data subjects. In some circumstances, the affected data subjects may require information made available in alternative formats (in particular: for those who are unable to access information digitally, those who are visually impaired or where English is not their first language).

33. A formal data breach notification must include the following information:

    a. the nature of the personal data breach

    b. the likely consequences of the personal data breach

    c. the measures taken or proposed to be taken to address the personal data breach

    d. the contact details of the organisation notifying of the breach

    In addition to the breach notification, you should prepare an FAQ document to anticipate likely questions from worried individuals. For example:

a. Precisely which items of my data have been breached?

b. Who has accessed my breached data?

c. Have you reported this breach to the Information Commissioner?

d. What steps can the data subject take, having now been notified? E.g. registering with Report Fraud, changing passwords, etc.

e. Where can they go for additional information? Do they know how to find that information? E.g. Government / Police press releases, NCSC web pages, etc.

f. For data subjects that are technologically inexperienced and are potentially vulnerable to further exploitation, what simple information do they urgently need to know up front? E.g. who they should contact if an external third-party approaches them about their data

g. You should make clear to data subjects what further communications are planned, from what accounts / numbers / addresses these will originate, and when they will take place. This will help protect the data subjects from some of that exploitation, e.g. phishing attacks using the breach as cover.

34. In the event of significant breach, what specific information should be included in the notification to data subjects must be carefully considered, advised by your SA, DPO, legal and organisational communications team, while balancing transparency and safety. Specific types of notification may cause further undue harm (e.g. tipping off a capable threat actor of a new vector of attack) or cause undue distress.

35. You should record (and subsequently be able to demonstrate) how your organisation has sought to mitigate harm to data subjects, which is likely to necessitate more than just notification e.g. establishing a helpline, providing identity monitoring tools, etc.

36. For highly sensitive notifications involving vulnerable data subjects, mitigations may also include the organisation coordinating proactively with the police or social services to implement additional measures to arrange welfare check ins or psychological support.

**Mitigating reputational damage**

37. You must make your organisational press office aware of the breach, and that it may become public. Before the press office issues any communications these should also be reviewed by your legal team.

38. Reputational damage is important, but it is not more important than affected individuals' wellbeing. Exposing data subjects to undue risks in the course of containing reputational damage is not acceptable in the strongest possible terms.

## Phase 4 - review following the incident - implementing lessons

39. The formal incident response process should include the activities as set out in this document, noting that these are recommendations and subject to local modification.

Once these have been completed, organisations should close the incident response. This does not mean that all activity will stop, but rather that any such activity has now become business-as-usual, even if only temporarily.

**Post-incident review and lessons learned**

40. You should conduct a comprehensive post-incident review of all incidents reported to the ICO. This would usually be led by the affect business unit and include, but not be limited to, an assessment of:

    a. How the breach occurred in the first place, specifically which processes went wrong and/or were not followed correctly.

    b. How long it took to identify the breach, and why (where applicable) there was a delay.

    c. Did the organisation's response follow the appropriate policies and processes.

    d. Did the organisation notify the data subjects, how was this perceived and what could be done to improve this in future.

    e. Where multiple organisations were involved, were there any obstacles to collaboration in jointly dealing with the breach.

    f. Whether appropriate processes were followed in recording, analysing, and reporting information.

    g. To what extent was legal advice incorporated in a timely fashion, e.g. in dealing with potential litigation, future compensation claims, etc.

41. Additional guidance is available within 'Principles for securing personal data in government services'. Critically, issues identified in the review must actually be acted upon and lead to tangible change. UK Resilience Academy has published The Lessons Management Best Practice Guidance in the effective management of lessons.

42. Always ensure the internal breach register is fully updated.

43. Report lessons learned, mitigations and updates on their implementation each quarter to the Government Data Protection Team within the Office of the Government Chief Data Officer in DSIT by contacting CentralGovDataProtection@dsit.gov.uk

**Maintain a central breach register**

44. In accordance with Article 33(5) UK GDPR, the breach must be added to your organisation's register of all incidents (regardless of severity) as soon as practically possible. The register serves various purposes, e.g. responding to queries, complaints and legal action from data subjects, interacting with regulators, identifying long-term themes and trends, etc. The register must record:

    - Cause - e.g. phishing, stolen device, misaddressed email, hidden data error etc.

- Data - e.g. specifics as to the data's nature, the quantity, the format, the number of data subjects, etc.
- Effects - the impact on data subjects.
- Remedial action (external) - what steps were taken to mitigate the impacts, both on your organisation and the data subjects.
- Remedial action (internal) - what steps has your organisation taken to prevent this from happening again?
- Rationale - in the event that reporting / notification to the ICO and data subjects wasn't done, what was the reason for this? *Note:* this will apply to less severe cases, as more severe cases come with statutory duties to report.

45. The organisation's security staff and DPO should review together the register periodically to identify systemic issues with the aim of addressing them. This will be accompanied by, and likely facilitated by, annual reporting to the organisation's Audit and Risk Committee (or equivalent).

46. Note that the ICO can request to audit an organisation's breach register to verify compliance with UKGDPR, Article 33 (5).