DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

TO: Secretary of State for Defence, Ministry of Defence

OF: Whitehall
London
SW1A 2HB
United Kingdom

I. INTRODUCTION AND SUMMARY

1. The Information Commissioner (the "**Commissioner**") has decided to issue the Secretary of State for Defence (represented by the government department of the Ministry of Defence, and therefore referred to interchangeably in this Penalty Notice as the "**MOD**") with a monetary penalty under section 155 of the Data Protection Act 2018 ("**DPA**") in respect of an infringement of the UK General Data Protection Regulation ("**UK GDPR**").

2. This Penalty Notice ("**Penalty Notice**") is given to the MOD pursuant to section 155 and Schedule 16 DPA.

3. This Penalty Notice sets out the reasons why the Commissioner has decided to require the MOD to pay a penalty, including the circumstances of the infringement and the nature of the personal data involved.

4. The Commissioner sent a Notice of Intent to the MOD setting out the reasons why the Commissioner proposed to give the MOD a penalty notice on 26 April 2023. The MOD submitted written representations to the Commissioner in response to the Notice of Intent on 7 September 2023 (dated 5 September 2023) and made representations orally at an oral hearing on 22 September 2023. This Penalty Notice takes into account the MOD's written representations and oral representations (together the "**Representations**") and, where appropriate, makes specific reference to them.

5. Having carefully considered the Representations, the Commissioner has found that the MOD has infringed Article 5(1)(f) UK GDPR (the "**infringement**") for the reasons set out in this Penalty Notice. In summary:

   a. The infringement involved serious deficiencies in the technical and organisational measures used by the MOD's Afghan Relocations and Assistance Policy ("**ARAP**") team in processing the personal data of individuals seeking relocation from Afghanistan. This failure left the security of personal data processed by the ARAP team at significant risk, in particular by way of disclosure through human error.

   b. As a consequence of the MOD not having appropriate security measures in place, personal data relating to 245 individuals was disclosed on 20 September 2021, putting their lives at risk (the "**20 September Incident**").

   c. The 20 September Incident involved the email addresses of these individuals being inadvertently placed in the "To" field of an email instead of the "blind carbon copy" ("**BCC**") field. Following this

incident, the MOD identified that two similar incidents involving the ARAP team had already occurred earlier in September 2021, also involving the inadvertent use of the "To" field rather than the BCC field. Overall, 265 unique email addresses were disclosed during the incidents.

6. The infringement lasted from at least 13 August 2021, being the date on which "Operation PITTING" was initiated, to 21 September 2021, being the date on which the MOD reported the 20 September Incident to the Commissioner.[1]

7. The Commissioner has issued this Penalty Notice in respect of the infringement on the basis that, in all the circumstances, and having regard to the matters listed in Articles 83(1) and (2) UK GDPR, a financial penalty is an effective, proportionate and dissuasive measure.

8. The Commissioner considers that the appropriate penalty to impose in respect of the infringement based on its nature, gravity and duration is £1,000,000. However, taking into account mitigating factors relating to the action taken by the MOD and the urgent and pressurised circumstances of the evacuation from Afghanistan, the Commissioner has decided to reduce the penalty to £700,000. In addition, the Commissioner has had regard to his policy in relation to enforcement against public sector bodies and decided to reduce the penalty by a further 50%. The penalty payable by the MOD is therefore £350,000.

[1] See paragraph 21 below for a timeline of events relating to the withdrawal from Afghanistan.

II. RELEVANT LEGAL FRAMEWORK

9. Section 155 DPA provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA, the Commissioner may, by written penalty notice, require the person to pay to the Commissioner an amount in sterling specified in the penalty notice.

10. The types of failure described in section 149(2) DPA include, at section 149(2)(a), "*where a controller or processor has failed, or is failing, to comply with … a provision of Chapter II of the UK GDPR … (principles of processing)*".

11. Chapter II UK GDPR sets out the principles relating to the processing of personal data that controllers must comply with. Article 5(1) UK GDPR lists these principles, and includes the requirement at Article 5(1)(f) UK GDPR that "*personal data shall be … processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". This is referred to in the UK GDPR as the "integrity and confidentiality" principle.

12. Article 5(2) UK GDPR makes it clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, [Article 5(1) UK GDPR]*". Article 24 UK GDPR sets out the responsibility of controllers to take appropriate steps to ensure and be able to demonstrate that processing is performed in accordance with the UK GDPR. This requires controllers to implement appropriate technical and organisational measures to ensure compliance, taking into account "*the nature, scope, context and purposes of processing as well as the risks of*

varying likelihood and severity for the rights and freedoms of natural persons".

13. Other relevant provisions of the UK GDPR and DPA are set out below in the sections dealing with the infringement by the MOD. The legal framework for setting penalties is set out in Section VI: 'Calculation of Penalty' below.

III. BACKGROUND TO THE INFRINGEMENT

14. This section summarises the circumstances of the failures that are the subject of this Penalty Notice for the purpose of providing the background to the finding of infringement. It does not seek to provide an exhaustive account of all the details of the events that have led to the issue of this Penalty Notice. As set out where relevant below, the Commissioner has taken into account the further information provided by the MOD in its Representations.

A. The personal data breaches reported by the MOD

15. The MOD is a ministerial department, led by the Secretary of State for Defence, tasked with ensuring the defence and security of the UK and its overseas territories. The MOD includes: (i) a Department of State, which is responsible for supporting Ministers, developing policy, developing and delivering plans, and generating military capability; and (ii) a Military Strategic Headquarters, that directs and carries out military operations on behalf of the government.[2]

[2] Details of the MOD's structures are set out within How Defence Works (September 2020) (publishing.service.gov.uk)

16. On 21 September 2021, the MOD reported a personal data breach to the Commissioner regarding an incident that had taken place on 20 September 2021 (referred to in paragraph 5 of this Notice, and hereafter, as the "**20 September Incident**"). The report confirmed that the MOD considered the 20 September Incident met the threshold to report a personal data breach.

17. The MOD reported to the Commissioner that "*over 200 e-mail addresses*" had been disclosed by the MOD's ARAP[3] team, which was stated to be a "*part of MOD*". The breach report confirmed that "*[a]n e-mail [had been] sent by a member of the ARAP team to individuals who [were] seeking assistance relocating from Afghanistan. This e-mail was sent to a distribution list, which was populated in the 'To' field. This allowed every member of the list access to the email address of other people on the email distribution list*".[4] The breach report stated that the affected individuals were "*claiming to be in a vulnerable situation in Afghanistan due to the recent withdrawal*".[5]

18. The MOD subsequently explained how the ARAP team operated at the relevant time.[6] ARAP "*is a Government policy 'owned' by the Cabinet Office under the National Security Council".* However, in practice the policy is "*administered by the MOD and Home Office*". Although, the ARAP was said to be "*owned*" by the Cabinet Office, the MOD explained that the MOD was required to comply with ARAP and that the MOD remained the controller for processing any personal data.[7]

[3] MOD Guidance, Afghan Relocations and Assistance Policy
[4] MOD Personal data breach report, 21 September 2021, p. 1-2.
[5] MOD Personal data breach report, 21 September 2021, p. 3.
[6] MOD letter to the ICO, 21 October 2021.
[7] MOD Third response to ICO questions, 6 June 2022.

19. The ARAP team was initially formed on 1 April 2021. It followed previous legacy resettlement work comprising the former intimidation policy (in place from 2010 to 2013) and ex-gratia scheme (in place between 2013 and 30 November 2022).[8] The ARAP team was administered as part of the MOD Permanent Joint Headquarters in Northwood, with some work also being carried out of the Embassy in Kabul, and initially generally processed the applications of a small numbers of Afghans who had worked for the UK Government in Afghanistan.[9]

20. The context for the 20 September Incident was the unusual and urgent circumstances of the withdrawal from Afghanistan and the fall of Kabul to the Taliban in summer 2021. The Commissioner accepts the MOD's description of the evacuation from Afghanistan as "*unprecedented in living memory*" and that the "*speed of the collapse was unexpected*".[10]

21. The timeline of events provided by the MOD makes clear how quickly events unfolded:

    a. In April 2021, the USA announced that it would be withdrawing troops from Afghanistan by 11 September 2021.
    b. On 15 April 2021, NATO, foreign and UK Defence Ministers confirmed the decision to start withdrawing all remaining forces from Afghanistan.
    c. In May and June 2021, the Taliban attacks began to intensify and the Taliban began to seize more territory.
    d. In June 2021, the Defence Minister and the Home Secretary announced that in recognition of the increased risk the relocation programme under ARAP would be accelerated.

[8] MOD Guidance, Afghan Relocations and Assistance Policy.
[9] MOD First response to ICO questions, 21 October 2021.
[10] MOD Representations, paragraphs 3(a) and 43(a).

e. Operation TORAL, the codename for the UK contribution to NATO's Resolute Support Mission in Afghanistan, drew to a close on 8 July 2021, alongside the withdrawal of other NATO forces.
f. The USA announced in July 2021 that its military mission in Afghanistan would conclude earlier than expected, by 31 August 2021.
g. During the first ten days in August 2021, the Taliban was reported to have committed several high-profile killings. The Taliban's actions included murdering the head of the Afghan government's media centre and an attempt to assassinate the Afghan government's acting defence minister.
h. By 8 August 2021, the Taliban had carried out a sweeping offensive through northern Afghanistan in a bid to encircle Kabul. Kunduz City, an area in northern Afghanistan that has routes to major cities including Kabul, was reported to have been largely in insurgent control by this date.
i. By 11 August 2021, hundreds of Afghan forces were reported to have surrendered to the Taliban in Kunduz. US officials speculated that the Afghan government could fall to the Taliban within 90 days. (In fact, the actual fall was far quicker.)
j. By 13 August 2021, the cities of Herat and Kandahar had fallen to Taliban control. The US military estimated that Kabul could soon succumb to insurgent pressure. On the same day, the UK military deployed again to Afghanistan to evacuate British nationals and eligible Afghans, referred to as Operation PITTING.
k. On 14 August 2021, the last major northern city, Mazar-i-Sharif, fell to the Taliban. This left only Kabul and Jalalabad remaining under Afghan government control. President Biden confirmed that he would not reverse the US decision to leave Afghanistan but said the US would deploy 5,000 soldiers to accelerate the removal of US diplomats and Afghan allies from the country.

l. On 15 August 2021, Kabul fell.

m. By 16 August 2021, the only territory under NATO control was Hamid Karzai airport.

n. Just before midnight on 28 August 2021, the last UK evacuation flight left Afghanistan carrying UK military personnel. Operation PITTING ended.[11]

22. After the last military flight left Kabul on 28 August 2021, the MOD began planning the removal of "*high risk and high priority*" individuals who had not made it out of Afghanistan. At that time, "*thousands of people eligible for relocation under ARAP remained in Afghanistan*". The MOD explained that "[redacted]".[12] The MOD stated that, at the end of August 2021, the ARAP team was receiving "*upwards of 3,000 emails a day from Afghans requesting to be recovered to the UK*".[13]

23. The MOD explained that the work of the ARAP team could be described as comprising four phases:

a. Pre-Operation PITTING (April 2021 to 13 August 2021);

b. During Operation PITTING (13 August to 28 August 2021);

c. Immediately post-Operation PITTING to the 20 September Incident (28 August 2021 to 20 September 2021); and

d. After the 20 September Incident (from 20 September 2021 onwards).[14]

[11] MOD Representations, paragraphs 32 to 41, 44 and 45.
[12] MOD Letter to the ICO, 16 December 2022.
[13] MOD First response to ICO questions, 21 October 2021, Q3(a) and MOD Representations, paragraph 47. As at 6 December 2022, 129,832 applications had been made under ARAP and as of 4 November 2022 around 6,000 people had arrived in the UK under ARAP (not including those evacuated during Operation PITTING) and another scheme called the Afghan Citizens Resettlement Scheme Pathway.
[14] MOD Representations, paragraph 50.

24. During the Pre-Operation PITTING phase, the team was small and included specialised trained selected staff based in Kabul and the UK.[15] Individuals seeking relocation were able to contact the MOD using a generic MOD email address. The number of individuals making applications was initially small and they were known to the ARAP team. The ARAP team contacted individuals on a one-to-one basis, in person (in Kabul), by telephone and one-to-one email.[16]

25. Operation PITTING led to a significant increase in demand on the ARAP team and its rapid expansion. The MOD has not been able to confirm the number of individuals in the ARAP team during this period, explaining that the urgent and unprecedented work meant that the MOD had to use any additional human resource that became available and that there was significant turnover in those working in the ARAP team.[17] At this time, the volume of applications significantly increased. The ARAP team was divided into smaller teams or cells to review emails, approve or deny applications, and advise eligible applicants on what they needed to do (for example, traveling to the airport and making contact with the UK contingent at the evacuee handling centre in Kabul).[18]

26. During Operation PITTING, the ARAP team began using group emails to send generic information to eligible approved applicants and to reject ineligible applicants, in addition to telephone and one-to-one email.[19]

[15] MOD Representations, paragraph 54.
[16] MOD Representations, paragraph 50(a).
[17] MOD Representations, paragraphs 55 and 56. The MOD explained that there were around 59 individuals on the ARAP team at the end of September 2021, but noted that this was not a consistent team and that it had been in flux following the end of Operation PITTING.
[18] MOD Representations, paragraphs 50(b) and paragraph 55.
[19] MOD Representations, paragraph 62.

27. In the period immediately after Operation PITTING the work continued to be urgent and the pressure on the ARAP team was intense. In addition to continuing to process applications, the ARAP team focused on maintaining continuous contact and providing support to eligible Afghans who had not been evacuated.[20] [redacted].[21] The Commissioner understands that the ARAP team sent the group emails to multiple addressees using the BCC function in Microsoft Outlook. However, as explained in this notice, the MOD did not have operating procedures and training in place for the ARAP team about how to send group emails securely until after the 20 September Incident.

28. The MOD explained that [redacted].

29. The 20 September Incident was the first incident involving the ARAP team that the MOD became aware of. On 6 June 2022, the MOD explained that the 20 September Incident involved the disclosure of 253 individual email addresses in an email that was sent to recipients using the "To" field, rather than these email addresses being placed in the BCC field.[22] As explained in more detail in paragraphs 53 - 56 below, there was some discrepancy in the MOD's reports about how many individual email addresses were compromised. However, the Commissioner

[20] MOD Representations, paragraph 50(c).
[21] MOD Representations, paragraph 63.
[22] MOD Fourth response to ICO questions, 6 June 2022, Q6. However the ICO notes that the MOD had previously and subsequently stated that there were 245 affected individual email addresses - see personal data breach report of 21 September 2021 p.3; MOD letter to ICO, 9 September 2022 p.2; and MOD letter to ICO, 16 December 2022, p1.

understands from other correspondence that the MOD accepts that the number of affected unique individual email addresses was 265, with some email addresses being disclosed more than once.[23]

30. All the individual email addresses were visible to all recipients of the email. The breach report stated that *"[t]here is no indication that the mailing list was intercepted by outside individuals, but the information that was shared could result in threat to life"*.[24] Similarly, an internal MOD data protection breach damage assessment report stated that the loss of data was "*significant*" and that *"[i]f this data was to fall into the wrong hands, either the Taliban or criminal organisations, it could almost certainly be exploited to target ARAP"*.[25] The MOD confirmed that two individuals "replied all" to the entire list of recipients. Of those two individuals, one provided their location and the other did not provide any additional information.[26] The MOD informed the Commissioner there was no indication that the information disclosed in the email had in fact been released beyond the distribution list – and the Commissioner has no evidence to suggest that this is not the case.[27] As explained further below, the MOD has subsequently submitted that the Commissioner has overstated the likely or potential impact of the incidents.[28]

31. Following the MOD's internal investigation and the Commissioner's inquiries, the MOD identified that two similar incidents had occurred earlier in September 2021 and subsequently notified these to the Commissioner:

[23] MOD, Response to Additional Questions submitted by the Information Commissioner's Office, 6 October 2023, Q2.
[24] MOD Personal data breach report, 21 September 2021, p. 4.
[25] MOD, 'ARAP Internal Incident Report (Partial) for release to ICO', p.1.
[26] MOD First response to ICO questions, 21 October 2021, Q16.
[27] MOD Third response to ICO questions, 11 January 2022, Q13.
[28] MOD, Representations, paragraph 3(e).

a. on 7 September 2021, an email was sent by a member of the ARAP team to 13 individual email addresses using the "To" field rather than the BCC field, meaning all email addresses were visible to all recipients (the "**7 September Incident**");

b. on 13 September 2021, another email was sent by a member of the ARAP team to 55 individual email addresses using the "To" field rather than the BCC field, meaning all email addresses were visible to all recipients (the "**13 September Incident**").

32. The 13 September Incident was reported to the Commissioner on 24 September 2021.[29] The MOD informed the Commissioner that the 7 September Incident had been detected locally (within the ARAP team) on 21 September 2021, but was not reported to the MOD's Data Protection Officer ("**DPO"**) at that time. The MOD discovered the 7 September Incident on 14 October 2021, when the MOD was contacted by a lawyer representing one of the affected individuals, and the MOD reported the breach to the Commissioner on 19 October 2021.[30]

33. After the 20 September Incident, the Secretary of State for Defence made a statement to Parliament on 21 September 2021 about the data breach and the MOD conducted an internal investigation to determine the extent and impact of the incident.[31] The Secretary of State for Defence made a further statement to Parliament on 15 November 2021, providing an update on the internal investigation.[32] The Secretary of State for Defence explained in his statement that the "*cause of [the incidents] was not simply human error in isolation, but a lack of standard*

[29] MOD Personal Data Breach report relating to 13 September Incident, 24 September 2021.
[30] MOD Personal Data Breach report relating to 7 September Incident, 19 October 2021.
[31] Data Breach: ARAP Applicants in Afghanistan - Hansard - UK Parliament, 21 September 2021, column 149.
[32] Afghan Relocations Assistance Policy Data Breach Investigation - Update, Statement made on 15 November 2021

operating procedures and training, which should have prevented such a mistake being made".

34. The individuals whose emails were contained in the distribution list were contacted by email using the BCC field, advised to delete the email, change their email address, and inform the ARAP team of their new contact details using a weblink provided by the MOD.[33] The MOD also amended the processes used by the ARAP team after the 20 September Incident by producing standard operating instructions that included specific guidance on the use of BCC and introducing a "second pair of eyes rule" for all bulk ARAP emails.[34]

B. The MOD's relevant policies and procedures

35. During the investigation, the Commissioner asked questions about the policies and procedures that the MOD had in place prior to 20 September 2021 that were relevant to preventing this type of incident, i.e. a personal data breach similar to the three incidents in September 2021.

36. The MOD confirmed that, at that time, it had an email-use policy set out within "JSP 441: Managing Information in Defence"[35], which provided advice to staff to consider when sending emails. This policy made no reference to the possible risks of recipients being able to see who else has received emails in certain circumstances where they should not. The MOD explained that JSP 441 was used to form "*a single digital policy environment*" within the MOD, and that the MOD does not require the

[33] MOD, 'ARAP Internal Incident Report (Partial) for release to ICO', p.1 and 'ARAP Email to recipients notifying of breach dated 20 September 2021'.
[34] MOD, 'ARAP Internal Incident Report (Partial) for release to ICO', p.1. See also MOD Representations, paragraph 69.
[35] A "JSP" is a Joint Service Publication, which is an authoritative set of policy documents that are specific to Defence, material to Defence outputs and have pan-Departmental applicability (see MOD, Representations, paragraph 12).

documentation of local policies by specific teams.[36] In other words, JSP 441 was a policy that covered the MOD's broader data handling for email usage generally, rather than specific guidance for the ARAP team. JSP 441 had two sections directly relating to email communications: "Managing Email Accounts" and "Sending, Receiving and Storing Emails".

37. The Commissioner requested information about how the relevant policies and procedures were brought to the attention of employees. The MOD told the ICO that "*[a] verbal brief was given to staff joining the ARAP team*". It further explained that there "*are also local security and data protection professionals whose role it is to promote security and data privacy awareness. On every user's desktop, there is a link to the JSP441 policy site which has 44 policy documents on the handling of personal data*".[37]

38. The Commissioner asked the MOD to provide details of any specific guidance in place for the use of BCC for sending group emails. The MOD explained that the JSP 441 policy set out guidance on how to send emails. In particular, among other things, JSP 441 reminded individuals to take care when sending emails, address them correctly, think about whether any security or privacy constraints may be breached before sending an email, and "*avoid multiple addresses (cc/bcc)*".[38]

39. The MOD also told the Commissioner that "*[i]ndividuals were also given a verbal briefing on how to use the BCC field in Microsoft Outlook*"[39]. However, the MOD has since confirmed in its Representations that this initial belief was not accurate and that "*[f]urther investigations by the*

[36] MOD Second response to ICO questions, 24 November 2021, Q9.
[37] MOD First response to ICO questions, 21 October 2021, Q9b.
[38] MOD Representations, paragraph 13.
[39] MOD First response to ICO questions, 21 October 2021, Q10.

MOD have revealed that (at the time of the date [sic] *incidents) there were daily verbal briefings, however, while there may have been a leadership expectation that a verbal briefing included bcc, the briefings given may not have expressly included the use of bcc*".[40]

40. The MOD was asked to provide evidence of the training undertaken by the staff members involved in the incidents in September 2021. The MOD explained that the "*MOD mandates that all staff are required to undertake the Defence Information Management Passport ("**DIMP**"). DIMP includes modules on data protection, data handling, electronic and physical security, and identifying information risk*".[41] The MOD confirmed that the members of staff involved in the incidents in September 2021 last completed the DIMP training in either September 2019 or January 2020, with such training being mandatory every three years.[42]

41. In terms of the technical and organisational measures in place to prevent personal data breaches, the MOD explained that:

> "*MOD personnel are mandated to undertaken* [sic] *data handling training to ensure they are aware of risks in personal data and identify appropriate actions to secure personal data and in the event of a data protection incident. MOD policy directs staff to be mindful of information they are sharing through e-mail. Individuals employed by MOD all undergo security vetting that is reviewed at regular intervals. Data Protection awareness videos are a mandated part of annual security briefs that take place at all MOD locations. There are specific software controls on Microsoft Outlook to prevent sensitive information being sent – however, in this case,*

[40] MOD Representations, paragraph 60(c).
[41] MOD First response to ICO questions, 21 October 2021, Q11
[42] MOD First response to ICO questions, 21 October 2021, Q11a; MOD Second response to ICO questions, 21 November 2021, Q12.

MOD personnel were not disclosing any sensitive material or personal data in their e-mails. The problem occurred as a result of the potential exposure of e-mail addresses".[43]

42. The MOD informed the Commissioner that, as a result of the incidents in September 2021, the MOD would develop enhanced data protection training and that a review of the mandatory training course (i.e. DIMP) was underway. The MOD also stated that it proposed to increase the frequency of when the training takes place, as well as a review of the content. In relation to the ARAP team, the MOD told the Commissioner that "*additional training and support materials have been provided to the ARAP team to increase their capabilities and limit the likelihood of further incidents*".[44] Since the 20 September Incident, the MOD has amended JSP 441 to include specific guidance on the use of BCC, produced specific data protection digital guidance for the Defence Operations team (which also covers the team responsible for setting up the ARAP team at the relevant time), developed Standard Operation Instructions for the ARAP team, and made changes to its data protection training programme.[45]

43. Following further questions asked by the Commissioner, the MOD provided additional information about the specific controls and policies the MOD had in place at the time of the incidents in September 2021 and the use of BCC.

44. The MOD explained that:

a. Although the MOD had enabled the capability within Microsoft Outlook that provides an alert or block when an attempt is made

[43] MOD First response to ICO questions, 21 October 2021, Q12.
[44] MOD First response to ICO questions, 21 October 2021, Q12.
[45] MOD Representations, paragraph 69.

to send sensitive information by email, the automatic protective marking did not identify the risk in relation to the emails that led to the incidents in September 2021 because they were brief and did not contain any identifiable sensitive information.[46]

b. The MOD's JSP 441 email policy is intended to cover all uses of email, and that the use of the BCC field was at the discretion of individual business units. Each business unit decides whether to use the BCC field, based on "*the nature of their business and the content of any communications*". In that context, the MOD "*refers to the Microsoft instruction on how to use BCC*".[47]

c. Neither the MOD, nor the ARAP team, had a general rule that emails should be sent out in bulk. This was a decision for the individuals involved in sending the emails. The MOD advised staff to exercise caution, but did not have a formal written policy that required the use of BCC.[48] The MOD generally discouraged the use of BCC during routine correspondence and would not normally require there to be specific guidance for the use of BCC for personnel. The MOD explained that "*this is because: (i) in normal operational contexts, it is important that email recipients are clear as to the identities of other recipients of that email, and (ii) … prior to the evacuation in Afghanistan, the MOD does [sic] not have a need to communicate by email with groups of the*

[46] MOD Second response to ICO questions, 24 November 2021.
[47] MOD Second response to ICO questions, 24 November 2021. The version of JSP 441 in place at the time of the 20 September Incident, did not make any reference to the use of BCC the field (see JSP 441, 17 December 2021). Following the opening of the Commissioner's investigation, JSP 441 was amended to provide guidance to mitigate the risk of similar personal data breaches occurring: "*Do not send emails that allow each recipient to see who else has received the email where security and privacy requirements demand each must not know of the existence of the other(s). Use either the blind courtesy copy (BCC) facility for the mailing list of recipients or send each individual their own separate copy. This will mitigate the risk of recipients receiving sensitive information which they have no right to see or using the reply all function to inadvertently send sensitive information to those who should not receive it.*" See: JSP 441, 11 March 2022.
[48] MOD Third response to ICO questions, 11 January 2022.

public outside the MOD on sensitive matters where it would be appropriate for their identities to be secret".[49]

d. The use of, or reliance, on the BCC field for sending emails was not common practice in the MOD. Individual business units may opt to use BCC in "*unique circumstances … for specific operational need*". However, the MOD does not require decisions to use BCC to be recorded and there was "*no expectation that a specific local process should be documented as it would represent an unnecessary level of bureaucratisation of the process*".[50]

45. The MOD decided to use Microsoft Outlook for the ARAP team to contact the individuals for potential relocation, having considered various options and taking into account the pros and cons. The MOD's decision to use Microsoft Outlook was based on balancing the security of the system and the ability to link to the MOD's main system, as well as the time-critical nature of the situation in Afghanistan. The MOD's view at the time was that other possible applications could not have been deployed as quickly or accessed as readily by the recipients of the emails. Further, it was not feasible to carry out the operation through oral or face-to-face contact, as would normally have been done and, as explained at paragraph 27 above, by mid-September 2021 it was no longer possible to use telephone contact.[51]

46. The MOD had a Data Protection Impact Assessment ("**DPIA**") in place for the processing activities of the ARAP team. However, as the team expanded significantly and faced increased demand following the

[49] MOD Representations, paragraph 14.
[50] MOD Fourth response to ICO questions, 6 June 2022.
[51] MOD Third response to ICO questions, 11 January 2022.

withdrawal from Afghanistan, *"a management decision was made to focus on the procedural aspects [of the operation] and work with the DPO team to have this revised"*. The MOD explained that the ARAP team and the DPO team *"discussed the risk of the operation with the management team but had understood the importance of not allowing the data protection impact assessment process to interfere with the urgent nature of the work".*[52]

47. In the Representations, the MOD has subsequently sought to clarify its general role in the evacuation of civilians from conflict zones and has emphasised that the role it played in Afghanistan was unique and unprecedented.

48. The MOD explained the secondary role which it would traditionally assume in such evacuations as follows:

"One role that the MOD performs which is partially outside of its primary defence role is the evacuation of civilians from conflict zones. The MOD has extensive experience of Noncombatant Evacuation Operations ("NEO") under an Overseas Assistance Request ("OAR"). A NEO is defined as: an operation conducted to relocate designated non-combatants threatened in a foreign country to a place of safety. The relevant policy document setting out the normal approach to NEO is the Joint Doctrine Publication 3-51: Non-combatant Evacuation Operations ("JDP 3-51") (3rd Edition dated March 2021). As explained in JDP 3-51 the Foreign, Commonwealth & Development Office ("FCDO") will lead on a NEO and the UK government discharges its responsibilities for the safety and security of British nationals overseas through the FCDO. The

[52] MOD Third response to ICO questions, 11 January 2022.

secondary role of the Military (and thus the MOD) is repeatedly emphasised in JDP 3-51:

> *'2.4.* ***Military in a subordinate and supporting role****. FCDO primacy is a key feature of a NEO. It is important for the balance of responsibilities between military and diplomatic/civilian staffs to be understood fully when planning and executing an evacuation.'"*[53]*.*

49. The MOD further explained the relationship between the FCDO and itself, as prescribed by the JDP 3-51, in identifying non-combatants who are eligible for evacuation by the UK, noting that in "normal circumstances" the FCDO would *"[l]ead and manage the process of identifying and contacting eligible persons; […] [w]ork closely with the appropriate UK representatives overseas […] ensuring the timely preparation and routine maintenance of crisis management plans; [and determine] (as far as possible and on a case-by-case basis) the numbers and locations of eligible persons […]*".

50. The MOD explained that it would, in "normal procedure", operate under the JDP 3-51 and offer support by "*[e]vacuating its own personnel and extracting eligible persons via an agreed military evacuation chain … [and] [w]here necessary, protecting eligible persons and FCDO staff during the evacuation process*".[54] The MOD explained that, prior to the evacuation in Afghanistan, it had always operated under the JDP 3-51 procedures. JDP 3-51 was not adopted in Afghanistan because of the unique circumstances of the evacuation, which included the Afghan National Army collapsing quicker than expected; uncertainty about the location and number of potentially eligible persons; the vast number of

[53] MOD Representations, paragraph 27.
[54] MOD Representations, paragraphs 29 - 31.

applications for evacuation being received daily by the ARAP team; and the uncertainty over how long Operation PITTING would continue.[55]

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

51. The Secretary of State for Defence, represented by the government department of the MOD, was the controller of the personal data of the individuals whose email addresses were disclosed in the 20 September Incident, and the other incidents in September 2021.[56] The MOD determined the purpose and means of processing that data within the meaning of section 3(4) DPA and Article 4(2) UK GDPR.

52. The MOD is established in the UK and the relevant processing of personal data took place in the UK.

B. Nature of the personal data involved

53. There was some inconsistency in the details provided by the MOD during the course of the Commissioner's investigation about the personal data that was the subject of the 20 September Incident and the 13 September Incident.

54. The MOD explained that the 20 September Incident involved the disclosure of 253 individual email addresses and the 13 September Incident involved the disclosure of 55 individual email addresses.[57] The

[55] MOD Representations, paragraphs 31 and 43.
[56] The MOD was a controller within the meaning of section 6 DPA and Article 4(7) UK GDPR. See MOD Third response to ICO questions, 11 January 2022 Q1.
[57] MOD Fourth response to ICO questions, 6 June 2022, Q6. Note that the MOD had previously indicated that 256 individual email addresses had been identified "between the two incidents" (MOD First response to ICO questions, 21 October 2021, Q19)

MOD told the ICO that the 55 email addresses included in the 13 September Incident were also included in the 20 September Incident.[58] Of these individual email addresses:

a. [redacted];
b. [redacted];
c. 55 included thumbnail photos of individuals; and
d. 23 included thumbnails of stock images.[59]

55. The MOD estimated that in "the worst-case scenario", 444 individuals could have been affected by the two incidents, if the dependents of the data subjects are also included.[60] The 7 September Incident involved the disclosure of 13 individual email addresses.[61]

56. The MOD subsequently confirmed that 265 unique email addresses were shared in the incidents. In some instances, the same email address was involved in more than one incident. At the time of the 20 September Incident, the individuals were understood to still be in Afghanistan and therefore at risk of reprisal. The MOD's Defence Afghan Relocations and Resettlement (DARR) Directorate [redacted][62], [redacted]

[58] MOD Fourth response to ICO questions, 6 June 2022, Q6. However, the MOD's earlier responses had indicated that 50 email addresses were affected in the 13 September Incident, of which 10 were identified as unique to that incident (MOD First response to ICO questions, 21 October 2021, Q27).
[59] MOD First response to ICO questions, 21 October 2021, Q19. The Commissioner notes that this breakdown indicates that 256 individual email addresses were affected.
[60] MOD First response to ICO questions, 21 October 2021, Q19 and MOD Fourth response to ICO questions, 6 June 2022, Q7.
[61] MOD Personal Data Breach report relating to 7 September Incident, 19 October 2021.
[62] The MOD is continuing to make every effort to relocate ARAP eligible persons as quickly as possible.

[redacted].[63]

57. The personal data disclosed included data that would allow for identification of persons who were seeking assistance relocating from Afghanistan.[64] This information is personal data within the meaning of Article 4(1) UK GDPR and section 3(2) DPA.

58. As the MOD accepted in its personal data breach reports, the data subjects were claiming to have some association with the MOD during the conflict in Afghanistan and the ARAP team's function and remit was concerned with "[redacted]".[65] In that context, the MOD has acknowledged that "[redacted]"[66] and "[redacted]".[67] It is self-evident that this data was particularly sensitive and required careful handling.

59. In its Representations, the MOD revised its position, somewhat downplaying the risks resulting from the disclosures and submitting that the Commissioner "*has overstated the likely or potential impact of the incidents and when considering the seriousness of them, failed to take into account material considerations*".[68]

[63] MOD, Response to Additional Questions submitted by the Information Commissioner's Office, 6 October 2023, Q2.
[64] Whether directly identifiable, i.e. via the inclusion of their name or photograph, or indirectly via other means such as other information which may be available.
[65] MOD response to ICO first inquiries, 21 October 2021, Q1.
[66] MOD Personal data breach report, dated 21 September 2021, p.4
[67] MOD, 'ARAP Internal Incident Report (Partial) for release to ICO', p.1.
[68] MOD Representations, paragraph 3(e).

60. While the MOD *"accepts that the incident does represent some degree of potential risk to the individuals"* and "*that this incident was serious in light of the circumstances in Afghanistan at the time",* the MOD's position is that:

a. [redacted];

b. [redacted];

c. [redacted];

d. [redacted]; and

e. only two individuals replied to the whole of the distribution list and, of those, only one provided reference to their location (at a high level, i.e. by reference to a city).[69]

[69] MOD Representations, paragraph 66. The MOD also "*maintains that no special category data was disclosed by the data incidents*". However, the Commissioner did not allege in the Notice of Intent that any special category data had been disclosed.

61. The MOD submitted that its position is supported by the fact that, to the best of its knowledge, there is no indication that any individual has experienced any actual harm as a result of the incident.[70] The MOD also submitted that "*it is relevant to note, that had the Taliban wanted to seek reprisals on those who had supported the Western forces they could have been identified during [the time when thousands of Afghans gathered around Hamid Karzai airport seeking to leave the country] by simply observing who were trying to leave*".[71]

62. As set out in the Notice of Intent, the Commissioner accepts that there is no evidence to suggest that the information disclosed was in fact released beyond the distribution list and that there is no evidence of actual harm being suffered by the individuals involved.[72] However, the Commissioner remains of the view that the nature of the personal data was of a type that was particularly sensitive and required careful handling in the circumstances. In particular:

a. [redacted]; and

[70] MOD Representations, paragraph 66(d).
[71] MOD Representations, paragraph 42. The Commissioner notes that elsewhere in its Representations the MOD submitted that that the period of Operation PITTING (13 August to 31 August) should be distinguished from the post-Operation PITTING period on the basis that during August 2021 "*there was an agreement in place with the Taliban to allow the free movement of all those who wanted to leave*" (MOD Representations, paragraph 71).
[72] Notice of Intent, paragraphs 28 and 99(a).

b. it appears reasonably unlikely that the Taliban, if they had suspected an individual of having worked for the UK, would have necessarily distinguished between an email from the MOD that demonstrated an individual was seeking relocation to the UK and one that specifically confirmed the individual's eligibility for relocation.

63. The Commissioner does not agree with the MOD's submission that the disclosure of 55 thumbnail photos of individuals can be ignored on the basis it constituted a "very small minority" within the overall number of email addresses involved.[73] In the circumstances, 55 thumbnail images still represents a significant number of photos. The Commissioner also notes the concerns voiced in Parliament about the gravity of the security breach and the Secretary of State for Defence's acknowledgement that, although the email addresses may not have all been individuals' full names, "*that does not change the fundamental impact that the email could have had and could still have*".[74]

64. The Commissioner's view is that, given the wider context of the data processing (i.e. as part of an operation to evacuate Afghans who had worked with the UK), the potential threat resulting from the unlawful disclosure of email addresses relating to 265 individuals is sufficient to find that the personal data involved was sensitive and required careful handling.

[73] These 55 photos were distinguished from the 23 thumbnails of "stock images" referred to in the MOD response to ICO first inquiries, 21 October 2021, Q19.
[74] Data Breach: ARAP Applicants in Afghanistan - Hansard - UK Parliament, 21 September 2021, column 150.

C. The infringement

65. The Commissioner has considered whether the facts set out above constitute an infringement of the UK's data protection legislation. In doing so, he has taken into account the MOD's Representations and makes reference to these, where relevant.

66. For the reasons set out below, the Commissioner's view is that the MOD has infringed Article 5(1)(f) UK GDPR. The infringement involved serious deficiencies in the MOD's technical and organisational measures used by the ARAP team in processing personal data of individuals seeking relocation from Afghanistan. As a consequence of the MOD not having appropriate security measures in place, the 20 September Incident led to the disclosure of personal data relating to 245 individuals, putting their lives at risk. Following this incident, the MOD identified that two similar incidents involving the ARAP team had already occurred, but had not previously been reported. Overall, 265 unique email addresses were disclosed using the "To" field rather than the BCC field in the three incidents.[75]

67. The Commissioner finds that the infringement lasted from at least 13 August 2021 (following the announcement of Operation PITTING), albeit the flaws in JSP 441 in terms of providing limited guidance on sending group emails securely predate this announcement, to 21 September 2021, being the date on which the MOD reported the breach to the Commissioner and began to implement measures to prevent a reoccurrence.

[75] MOD, Response to Additional Questions submitted by the Information Commissioner's Office, 6 October 2023, Q2.

68. The MOD, in its Representations, has disputed the Commissioner's finding regarding the duration of the infringement, stating its position that "*the relevant period should only be from the date when it was necessary to move to only email communication communications [sic], necessitating a greater reliance on email, rather than telephone calls to provide support; that decision was taken in mid-September 2021*".[76] The Commissioner disagrees and maintains that the infringement lasted from at least 13 August 2023 on the basis that the MOD should have had appropriate measures in place for sending group emails and using BCC by at least this time. As the MOD stated in its Representations, group emails began to be used during Operation PITTING[77] and the Commissioner notes that, in any event, the incidents on 7 September 2021 and 13 September 2021 preceded mid-September 2021.

69. The Commissioner also takes the view that the 20 September Incident was caused by a longer standing failure to put in place appropriate measures for the ARAP team to follow, not a specific failure to put in place measures at the time the MOD decided to stop using telephone communications in mid-September 2021.

70. The measures the ARAP team had in place to ensure the security of the personal data sent using email comprised the MOD-wide email policy set out in JSP 441. On 24 August 2021, the deputy DPO for the MOD sent an email to the Chief of Staff of the Operation PITTING Policy team rightly identifying that "*there needs to be a focus on security measures in place to protect the personal data*" and asking "*[h]ow are we sharing the information within and outside the MOD? Is this done securely?*".[78]

[76] MOD Representations, paragraph 71.
[77] MOD Representations, paragraph 62.
[78] MOD Letter to ICO, 16 December 2022, Annex 1.

71. However, the MOD's policies and procedures in place for the ARAP team had significant shortcomings, taking into account the sensitive nature of personal data of the individuals seeking relocation from Afghanistan. In particular, as set out in more detail above in paragraphs 35 - 50:

    a. The MOD did not have in place specific processes or guidance for the ARAP team in using group emails to contact individuals outside the MOD in Afghanistan.

    b. The ARAP team relied on the MOD's broad email usage policy set out in JSP 441 and, although new members of the ARAP team were given some initial support and received verbal briefings, the MOD has confirmed that this "*may not have expressly included the use of bcc*".[79]

    c. Before the amendments put in place following the 20 September Incident, JSP 441 did not contain guidance about the use of the BCC field when sending group emails or, more generally, about the process that should be followed when sending emails to a large number of recipients securely.

72. The MOD submitted that the measures it had in place were appropriate on the basis that it had "*no ordinary organisational need to use bcc, and indeed its use is discouraged*".[80] As set out in paragraphs 47 - 50 above, the MOD explained that official policy in JDP 3-51 on civilian evacuation makes clear it is for the FCDO to be responsible for identifying and contacting eligible persons, not the MOD. The MOD submitted that it was therefore reasonable for the MOD not to have organisational measures

[79] MOD Representations, paragraph 60. During the period of investigation that led to the Notice of Intent the MOD told the ICO that "[i]ndividuals [joining the ARAP team] were … given a verbal briefing on how to use the BCC field in Microsoft Outlook" (see paragraph 39 above).
[80] MOD Representations, paragraph 73(a).

in place on an issue that could not reasonably have been foreseen, such as – in this case – using group email to contact individuals seeking relocation from Afghanistan.[81]

73. While the Commissioner accepts that the events in Afghanistan in 2021 were unprecedented and that the MOD was operating outside of its usual role (as defined in JDP 3-51), the Commissioner remains of the view that the measures the MOD had in place, including the limited guidance in JSP 441 on exercising caution and discouraging the use of BCC when sending emails, were inadequate.

74. The inadvertent use of the "To" or carbon copy (**"CC"**) fields rather than BCC field in Microsoft Outlook to insert email addresses for bulk communications has, for some time, been a well-known security risk.[82] It is a risk that the MOD should have been well aware of in the light of the fact that its personnel are on occasion required to be diverted to urgent work (including national and international emergencies) involving the evacuation of civilians and requiring a rapid response dealing with unfamiliar matters. The Commissioner therefore considers that security risks associated with inadvertent disclosure when using BCC to send group emails is something the MOD ought to have foreseen, either when establishing the procedures for the ARAP team to use in making contact with individuals in Afghanistan, or at the very least when group emails started to be use during Operating PITTING.

75. Although the MOD was placed in an unfamiliar position in being specifically required to lead on identifying eligible individuals in the circumstances of Operation PITTING, the MOD's role in assisting with

[81] MOD Representations, paragraph 73(a).
[82] For example, see the previous decisions of the Information Commissioner referred to in paragraph 155 below.

such evacuations was not unprecedented. Indeed, the MOD explained that it has extensive experience of Noncombatant Operations under an Overseas Assistance Request[83] and the Commissioner understands that in relation to Operation PITTING the MOD worked closely with FCDO colleagues, drawing on their collective experience and knowledge of how best to contact Afghans in the circumstances.[84]

76. The fact that the ARAP team sent group emails using BCC as a matter of practice – albeit with a lack of standard operating procedures and training on security of email communications – indicates that members of the ARAP team foresaw there was need to handle the personal data of the individuals in Afghanistan with some degree of sensitivity and take steps to avoid it being compromised. Unfortunately, the lack of measures in place for the ARAP team to address the foreseeable risks of inadvertent disclosure when using BCC were insufficient to prevent the data incidents occurring.

77. The MOD submitted that, in the urgent circumstances of Operation PITTING and its aftermath, it was not reasonable to expect the MOD to slow or pause the process of contacting potentially eligible persons, with the subsequent potential risk to life of any delay, while additional training was provided or written policies and guidance signed off.[85] The MOD further submitted that it "*relies on the expert views of military professionals that any delay in the work of the ARAP team could have resulted in loss of life*" and "*does not understand on what basis the [Commissioner] could reasonably challenge that assumption in the circumstances*".[86]

[83] MOD Representations, paragraph 27.
[84] MOD, Response to Additional Questions submitted by the Information Commissioner's Office, 6 October 2023, Q1.
[85] MOD Representations, paragraph 73(c).
[86] MOD Representations, paragraph 74.

78. The Commissioner accepts that delays in the ARAP team's work could have put lives at risk. However, the Commissioner considers that poor security measures leading to the disclosure of sensitive information about those seeking evacuation from Afghanistan could also, and indeed did in practice, put lives at risk. The MOD was aware that the data relating to individuals seeking relocation being handled by the ARAP team included high risk data (such as the identities of individuals who may be in vulnerable positions). In such circumstances, the MOD should have had a policy in place properly addressing this risk and it would have been proportionate for it to have done so, given the severity of the potential harm to the Afghans seeking relocation.

79. The MOD submitted that the Commissioner's characterisation misunderstands or oversimplifies the position.[87] The MOD stated that it was aware that the personal data needed to be handled sensitively (which was why the ARAP team was planning to work with one-to-one email, face-face-contacts and by telephone location tracking), but did not predict how quickly the Afghan government would fall, "*resulting in the MOD needing to rely on emailing such substantial numbers of individuals*".[88] In that context, the MOD suggests that the Commissioner's approach is "not proportionate" and means the MOD would have needed to "*have in place multiple plans each with the relevant data processes guidance and training provided to address every possible, but unlikely, scenario for the ARAP team*".[89]

80. The Commissioner disagrees. His expectation is not that the MOD needed to have "multiple plans". Rather, his expectation is that, as required by

[87] MOD Representations, paragraph 80.
[88] MOD Representations, paragraphs 82 to 83.
[89] MOD Representations, paragraph 83.

Article 5(1)(f) UK GDPR and taking into account the severity of the risks facing Afghans seeking relocation if their data was disclosed, the MOD should have put in place a more secure means of sending group emails and provided guidance to staff in ARAP about how to mitigate the risks involved. This could have been achieved through relatively simple and proportionate measures, taking into account the nature of the circumstances. For example, even if the MOD was unable to introduce a software solution in the time available to send emails to multiple recipients without using BCC (which would have been preferable), it would have been straightforward to provide clear guidance to members of the ARAP team about the risks of relying on BCC for sending group emails securely and to mitigate that risk by introducing a "second pair of eyes rule" (as the MOD did following the 20 September Incident).[90] Contrary to the MOD's submissions, implementing operating procedures and guidance for the ARAP team that addressed the risks of using BCC could have been done quickly and with limited disruption to its work.

81. Further, as the MOD has acknowledged, the "*risks arising from the change in how officials communicated with applicants – which had previously been done on an individual basis, and often by telephone rather than email – were not fully recognised due to the urgency and the speed of the situation*".[91] In the Commissioner's view these risks should have been recognised and managed, notwithstanding the highly pressurised circumstances. Steps should have been taken to ensure that members of the ARAP team were made aware of the risks of sending group emails to reduce the risk of human error (both during Operation PITTING and the period immediately after). However, the evidence

[90] The MOD submitted that "*additional checks and balances, such as a 'second pair of eyes' approach … would lead to failure to work as quickly as is required in such urgent, life-or-death circumstances. Doing so could prevent loss of competitive advantage over our adversaries, and ultimately, increase risks to or, in extreme circumstances, loss of life*" (see MOD Representations, paragraph 97). The Commissioner's view is that a failure to properly protect sensitive data can also put lives at risk.
[91] MOD Second response to ICO questions, 24 November 2021, Q5.

indicates that the MOD did not address the risks by providing specific guidance about the risks of sending group emails and, in particular, reliance on BCC.

82. The MOD's Representations suggest it believes it was reasonable not to have done so because of the urgency and pressure under which the ARAP team was working.[92] In that regard, the MOD noted that its internal investigation following the 20 September Incident "*found several contributing factors which contributed to the data incidents, all arising from the intense speed, scale and operational pressures, and the fact the team had been built and then expanded quickly to support the rapid and unforeseen increase in urgent activities*".[93] The Commissioner does not dispute that these factors are likely to have contributed to the data breaches. However, the Commissioner notes that the MOD's Representations do not also refer to the fact that, as the Secretary of State for Defence explained to Parliament, "*[t]he cause of these mistakes was not simply human error in isolation, but a lack of standard operating procedures and training, which should have prevented such a mistake being made*" and that "*the individuals' actions that contributed to the data breaches were not found to have been deliberate or negligent, but the result of insufficient training and data handling procedures*".[94]

83. The Commissioner considers that the urgency and pressure of the situation made it even more important that risks relating to the ARAP team sending group emails to at risk individuals in Afghanistan were properly mitigated by the MOD having an appropriate policy in place. As the MOD states, "*[t]he likelihood of human error occurring, it must be recognised, is also increased when individuals are working under intense*

[92] MOD Representations, paragraph 90.
[93] MOD Representations, paragraph 68.
[94] See paragraph 33 above.

pressure and in unforeseen circumstances".[95] The Commissioner agrees. The MOD should have had appropriate measures in place to avoid the risks of disclosure when sending group emails. Without them, the urgency of the situation and the danger of reprisal meant there was a severe risk to the individuals seeking evacuation if their information fell into the wrong hands and – as borne out in practice – a high risk of human error on the part of the ARAP team when working under such pressure.

84. Although the MOD had guidance in place for sending and receiving emails (within the broader JSP 441 policy), which included the need generally to exercise caution when sending emails, this guidance failed to address the issue of security around the sending of bulk emails to multiple recipients outside the MOD.

85. As explained in paragraphs 38 and 44.c) above, the JSP 441 policy was designed to discourage the use of BCC by telling MOD staff to "*avoid multiple addresses (cc/bcc)*". The primary reason for this policy was that the MOD wanted to ensure that the recipients of emails were aware of who else had received it. The MOD submitted that, because in "*the MOD's normal business bcc is actively* discouraged" (emphasis in original), it was reasonable not to provide the ARAP team with specific guidance on the use of BCC (or indeed other security measures for sending group emails) in order to protect the personal data of individuals seeking to be evacuated from Afghanistan.[96] The Commissioner's view is that not only was the guidance in JSP 441 inadequate, it set out the of opposite of the guidance needed by the ARAP team in circumstances where there was no alternative available to the ARAP team other than using CC or BCC for sending group emails. The ARAP team needed measures in place to

[95] MOD Representations, paragraph 90.
[96] MOD Representations, paragraph 75(a).

ensure group emails were sent securely in a way that recipients did not know who else was being contacted at the same time. This need was not covered by JSP 441.

86. The guidance within JSP 441 was intended by the MOD to provide a "*single digital policy environment*" and therefore applied broadly across the MOD. Rather than implementing guidance as to the use of the BCC field for group emails, or taking some other security measure in relation to group emails sent externally, it was instead "*left to the discretion of business units*" (such as the ARAP team) to decide on the course of action, under the supervision and monitoring of the MOD's Data Protection Officer's Team ("DPOT").[97] In the circumstances, that guidance was insufficient for the purpose of Article 5(1)(f) UK GDPR in ensuring that appropriate security measures were in place for the ARAP team.

87. As set out in paragraph 45 above, the MOD appears to have given some consideration to the means of email communication used to contact individuals seeking relocation from Afghanistan. Taking into account the urgency of the situation, as well as other factors, the MOD decided to use Microsoft Outlook. However, the MOD should have recognised the inherent risks in relying on Microsoft Outlook and the BCC field for communicating with multiple recipients using group emails, particularly given the high-risk nature of the situation involving the relocation of individuals from an area of conflict. The MOD submitted that it did recognise the risks of using of using Microsoft Outlook to send group emails, which is why it planned for the ARAP team to make contact with

[97] MOD Second response to ICO questions, 24 November 2021, Q8. MOD Representations, paragraph 84.

individuals by telephone, face-to-face contact and individual email during Operation PITTING.[98]

88. The Commissioner accepts that the speed at which the Afghan government collapsed was a surprise. However, he notes that the MOD started using group emails during the period of Operation PITTING itself (not only once security risks meant the telephone system was no longer safe from mid-September) and considers that, having decided to use email to contact individuals in a conflict zone where there was a clear risk of unexpected developments and given the volume of emails being received, it should have been foreseeable that the ARAP team may need to contact larger groups of people quickly. The Commissioner's view is that the MOD should have been better prepared by putting in place an alternative and more appropriate method of sending group emails to the individuals in Afghanistan, for example using software capable of sending individual emails to multiple recipients (or even using the "Mail Merge" function available within Microsoft Outlook).[99] Had the ARAP team used an alternative method then the incidents in September 2021 may have been avoided.

89. The Commissioner's position is that the MOD ought to have foreseen the risks of using BCC and already had software in place for sending group emails securely. However, the Commissioner accepts that in the specific context of Operation PITTING, having chosen to use Microsoft Outlook, it would have been difficult for the MOD to procure and roll out alternative software to send group emails given the urgency of the situation in Afghanistan. Notwithstanding that, as set out above, the Commissioner's view is that other steps still should have been taken to

[98] MOD Representations, paragraph 86.
[99] The MOD confirmed at the oral hearing that Mail Merge was available, but would have required additional training to use.

ensure members of the ARAP team were made aware of, and were therefore better placed to mitigate, the security risks of sending group emails using Microsoft Outlook and relying on BCC.[100]

90. While, as made clear in this notice, the Commissioner accepts the circumstances of Operation PITTING were unusual and highly pressurised, he considers that the MOD's Representations overstate the difficulty of putting appropriate measures in place for the ARAP team and the time that would have been required to do so. Further, the MOD could have taken action quickly once it became clear that the ARAP team would need to send group emails to individuals seeking relocation by quickly putting in place operating procedures and guidance to mitigate the risks of using BCC. However, as the Secretary of State for Defence put it in his statement to Parliament in November 2021: "*In the haste of this transition the risks arising from changing how officials communicated – which had previously been done on an individual basis, often by telephone rather than email – were not fully recognised or managed*".[101]

91. The Commissioner's view is that implementing such procedures and guidance would have been a straightforward task that would have significantly reduced the risk of inadvertent disclosure (and therefore the potentially severe risks to individuals in Afghanistan of such disclosure), while also not materially slowing down the evacuation. Indeed, following the 20 September Incident, the MOD amended its email use policy, which

[100] The Commissioner notes that he is not alone in having concerns about the way the MOD approached sending group emails. For example, during debate in the House of Commons relating to the data breach on 21 September 2021, parliamentarians suggested that "*surely it would not be too difficult to have an automated reminder or check, if it looks as if an email of a sensitive nature is going to be sent to multiple recipients*" and "*pretty much every MP uses a caseworker system, a piece of simple software that costs a few hundred pounds per year which ensures that mistakes of this nature cannot happen*" (see: Data Breach: ARAP Applicants in Afghanistan - Hansard - UK Parliament, 21 September 2021, column 155).

[101] Afghan Relocations Assistance Policy Data Breach Investigation - Update, Statement made on 15 November 2021.

was updated to include the following text that specifically addressed the risks of using BCC:

> "*do not send emails that allow each recipient to see who else has received the email where security and privacy requirements demand that each must now know of the existence of the other(s). Use either the blind courtesy copy (BCC) facility for the mailing list of recipients or send each individual their own separate copy. This will mitigate the risk of recipients receiving sensitive information which they have no right to see or using the reply all function to inadvertently send sensitive information to those who should not receive it*".[102]

92. In addition, as noted above in paragraph 34, after the September 20 Incident the MOD implemented a "second pair of eyes" policy for the ARAP team when sending emails to multiple external recipients. Such a procedure provides a double check whereby an email instigated by one member of staff is cross checked by another. The MOD submitted that "*it was not possible to introduce this policy earlier [than October 2021] because of the volume of correspondence being sent and the urgency of the work relating to Operation PITTING*". However, it is not clear to the Commissioner why a simple and relatively quick check with a colleague to ensure that email addresses had been placed in the BCC field rather than the "To" or CC fields would not have been a proportionate measure to avoid the significant risks of inadvertent disclosure of sensitive information likely to put lives at risk.

93. The MOD also informed the Commissioner that it has also accredited the use of a "*secure file transfer solution that allows sharing of sensitive*

[102] JSP 441, Sending and receiving emails, last modified 11 March 2022.

information through a secure browser-based customer contact portal", thereby removing the reliance on the use of BCC[103] and is implementing rules within Microsoft Outlook to warn email senders when they use the CC field as a further protective measure.[104]

94. The policy changes since the 20 September Incident – in particular, amending JSP 441 to include specific guidance on the use of BCC and using a "second pair of eyes" check – are precisely the measures that (in the absence of using a bulk email service or mail merge service) should have been put in place before, or at the very least once, the ARAP team started to send group emails to Afghans seeking evacuation and which could have prevented the incidents.

95. The MOD's failures in relation to its lack of compliance with Article 5(1)(f) UK GDPR are underlined by the fact that, following the report of the 20 September Incident, it discovered that there had been two almost identical incidents in the preceding fortnight: the 7 September Incident and the 13 September Incident. It is particularly concerning that, despite the MOD's internal investigations, the 7 September Incident did not come to light until over a month later when it was brought to the MOD's attention.[105] If the MOD had had appropriate technical and organisational measures in place then it may have identified the 7 September Incident, which involved the disclosure of personal data to fewer recipients than either the 13 September Incident or the 20 September Incident, and would have been able to implement steps to avoid the same thing happening twice more in September 2021.

[103] MOD Third response to ICO questions, 11 January 2022, Q2.
[104] MOD, Response to Additional Questions submitted by the Information Commissioner's Office, 6 October 2023, Q2.
[105] See paragraph 32 above.

96. The MOD submitted that it is wrong for the Commissioner to take the failure to identify the two earlier data breaches into account when considering whether there has been an infringement of Article 5(1)(f) UK GDPR on the basis that (i) the Commissioner has underestimated the extraordinary urgency and pressure on the work of the ARAP team and (ii) data breaches can occur and be undetected through human error even where there are appropriate organisational measures in place.[106]

97. As made clear in this notice, the Commissioner fully appreciates the urgency and pressure on the work of the ARAP team. He also acknowledges that data breaches can occur as a result of human error despite a controller having appropriate measures in place. However, in the specific context of this case, the Commissioner considers that risks arising from the disclosure of information relating to individuals seeking relocation from Afghanistan and the severity of the potential consequences, including risk to life, were such that the MOD should have been especially vigilant in identifying any data breach to ensure the failure was not repeated. Further, as explained at paragraph 83 above, the increased likelihood of human error occurring in an urgent and pressurised situation meant that the MOD should have taken greater care to ensure the appropriate security measures were in place for sending group emails.

D. Section 26 Exemption for national security and defence purposes

98. Section 26 DPA provides for an exemption from certain provisions of the UK GDPR if exemption from the provision is required for the purpose of safeguarding national security or for defence purposes (the "**Section 26 Exemption**"). The provisions to which such an exemption may apply are

[106] MOD Representations, paragraph 90.

set out in section 26(2) DPA and include "*Chapter II of the UK GDPR (principles) except for (i) Article 5(1)(a) (lawful, fair and transparent processing), so far as it requires processing of personal data to be lawful; (ii) Article 6 (lawfulness of processing); and (iii) Article 9 (processing of special categories of personal data)*".

99. Accordingly, the exemption would apply to Article 5(1)(f) UK GDPR if that exemption is required for the purpose of safeguarding national security or for defence purposes. However, as set out in the ICO's guidance, "*this is not a blanket exemption*" and a controller "*must be able to show that the exemption from specified data protection standards is required*".[107] When deciding whether the exemption applies, a controller should therefore consider the actual consequences for the relevant national security or defence purposes if it had to comply with the UK GDPR.

100. The ICO's guidance is consistent with the Parliamentary debate relating to the intended application of the Section 26 Exemption for defence purposes. During the committee stage of the passage of the DPA, Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins MP), answering questions on behalf of the UK Government, confirmed that "*this is not a blanket exemption. The high threshold can be met only in very specific circumstances*".[108]

101. The Parliamentary Under-Secretary of State further explained that:

    a. *"[o]nly where a specific right or obligation is found to incompatible* [sic] *with a specific processing activity being*

[107] ICO Guide to UK GDPR, National security and defence.
[108] Hansard, Data Protection Bill Committee, 15 March 2018, Column 109.

undertaken for defence purposes can that right or obligation be set aside"; and

b. "*[t]he application of the exemption should be considered only in specific cases where the fulfilment of a specific data protection right or obligation is found to put at risk the security, capability or effectiveness of UK defence activities*".[109]

102. The MOD's own internal guidance similarly makes clear that the Section 26 Exemption is "*not a blanket exemption*" and only applies in certain circumstances where national security or defence would otherwise be undermined:

> "*If […] the rights or obligations that [MOD] is expected to meet [under UK GDPR] might present a risk to national security, you should consider if an exemption from the GDPR is 'required for the purpose of safeguarding national security'. […] In this context, 'required for' means when it is reasonably necessary. This means the 'national security' exemption is not a blanket exemption and cannot be applied to all personal data processed by MOD at all times. Instead, the exemption should only be applied when meeting a specific data protection right or obligation could potentially undermine national security. MOD must consider all the circumstances of the case in such an event*".[110]

103. It is a question of fact as to whether the Section 26 Exemption is required in the relevant circumstances to ensure that meeting a specific data protection right or obligation does not undermine national security or defence purposes.

---

[109] Hansard, Data Protection Bill Committee, 15 March 2018, Column 108.
[110] MOD Letter to ICO, 16 December 2022, paragraph 11.

104. The MOD submitted that the Section 26 Exemption applied to the processing of personal data by the ARAP team "*for the short and compelling reason that to focus on technical and organisational measures in these circumstances would have diverted time and personnel away from operational matters of unprecedented and unforeseen urgency, which would in turn have created real risks to life and to the effectiveness of this evacuation operation*".[111]

105. The MOD further submitted that:

    a. the work of the ARAP team, including its email activities, was integral to matters of defence and national security;

    b. the use of group emails was "*necessary to contact large groups of eligible persons to provide them with information on and enable their evacuation from a conflict zone*";

    c. requiring the MOD to comply with Article 5(1)(f) would have been prejudicial to the effective pursuit of the ARAP team's objectives because the MOD "*cannot be expected to divert its focus from core defence and security actions towards ensuring data security measures imposed by the UK GDPR are complied with*";

    d. additional checks and balances would "*lead to a failure to work as quickly as is required in such urgent, life-or-death circumstances*"; and

[111] MOD Representations, paragraph 92.

e. if the data security duty applied with the prospect of ICO enforcement then it "*would likely create a more risk-averse culture among those working in contexts such as [the ARAP team]*", which would "*likely lead to fewer individuals putting themselves forward for such roles*".[112]

106. The Commissioner has considered the MOD's representations in respect of the Section 26 Exemption, and accepts that what is "required" for safeguarding national security and defence is principally a matter for the MOD, rather than Commissioner, to decide.[113] However, the Commissioner's view remains that the Section 26 Exemption does not apply to exempt the MOD from all of the requirements of Article 5(1)(f) in the specific circumstances of this case. As explained above, the MOD handled personal data in such a way as to put at risk the lives that the MOD was seeking to protect. The measures in place (which the MOD has accepted applied to the handling of data by the ARAP team in this operation) were both plainly insufficient for the purpose of Article 5(1)(f) and for protecting the security of the individuals seeking relocation from Afghanistan.

107. The Commissioner disagrees with the MOD's position that the objectives of national security and defence could not be achieved without prejudice to data protection law in the circumstances of this case.[114] In the circumstances of the work of the ARAP team, the requirements of Article 5(1)(f) UK GDPR were clearly complementary to the interests of national security and defence in ensuring that appropriate measures were in place to protect the personal data of Afghan civilians who, as the MOD accepts,

[112] MOD Representations, paragraphs 94 to 98.
[113] The Commissioner notes the MOD's reference to Secretary of State for the *Home Department v Rehman* [2003] 1 AC 153 as authority that in circumstances relating to national security significant weight should be afforded to the views of the executive (MOD Representations, paragraph 100).
[114] MOD Representations, paragraph 99.

"*were assessed to be at high and imminent risk of threat to life requiring their relocation to the UK*".[115]

108. The MOD submitted that it is also not possible to reconcile the need to focus on critical defence and security objectives with "*ensuring that data security measures imposed by the UK GDPR are complied with, for example, by tailoring new email security policies, procuring new systems, and scoping out and ensuring that other appropriate training and monitoring are in place to achieve adherence to those systems and policies*".[116] The Commissioner disagrees and considers that the MOD overstates in its Representations the scope of the measures the Commissioner would expect to have been in place for the ARAP team in what the Commissioner accepts were urgent and pressurised circumstances. As set out in paragraphs 90 - 91, the MOD could have taken action quickly once it became clear that group emails would be sent to Afghans seeking relocation, as it did after the 20 September Incident.

109. Finally, the Commissioner would be concerned if the creation of a "*more risk averse culture*" in relation to information security was reason for exempting the MOD or others from applying the requirements of Article 5(1)(f) UK GDPR in circumstances where it is also important for national security and defence purposes for the personal data in question to be properly protected.

V. DECISION TO IMPOSE A PENALTY

110. For the reasons set out below, the Commissioner has decided to impose a penalty of £700,000 on the MOD in respect of the infringement of

[115] MOD Representations, paragraph 96.
[116] MOD Representations, paragraph 96.

Article 5(1)(f) UK GDPR. However, taking into account the fact the MOD is a government department and therefore a public body, the Commissioner has decided that it is appropriate to reduce the amount of the penalty by 50% to £350,000.

A. Legal Framework – penalties

111. When deciding whether to issue a penalty notice to a person and determining the appropriate amount of that penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, so far as they are relevant in the circumstances of the case.

112. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate, and dissuasive in each individual case.

113. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

> (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
> (b) the intentional or negligent character of the infringement;
> (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
> (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

B. The Commissioner's decision on whether to impose a penalty

114. The Commissioner has considered the factors set out in Articles 83(1) and 83(2) of the UK GDPR in deciding whether to issue a penalty. For the reasons given below, he is satisfied that, in all the circumstances, the infringement is sufficiently serious to justify issuing a penalty and that doing so is effective, proportionate and dissuasive. In making his assessment, the Commissioner has taken into account the MOD's Representations that it would be inappropriate for him to issue a penalty.

115. The MOD submitted that the Commissioner imposing a monetary penalty in this case would be unwarranted and disproportionate. The MOD's

Representations on the penalty are addressed, where relevant, in more detail below. However, in summary, the MOD submitted that:

a. A fine is not necessary to dissuade the MOD from future mistakes and it is not proportionate for the Commissioner to issue a fine to dissuade others.

b. Issuing a penalty notice is inconsistent with the ICO's Regulatory Action Policy, including because "*the incidents were not wilful, deliberate or negligent: they were the result of human error and an intense and urgent environment … not part of a systemic failure by the MOD*".

c. A fine would be disproportionate and ineffective for a range of other reasons, as set out where relevant in the Commissioner's assessment below.[117]

(a) <u>the nature, gravity and duration of the infringement</u>

116. This was a significant infringement of Article 5(1)(f) UK GDPR. The processing of personal data relating to data subjects in a conflict zone for the purpose of their extrication is of a highly sensitive and delicate nature. The data subjects involved were "*in a vulnerable situation in Afghanistan*" and were at "*extreme risk of reprisal from the Taliban*" because of their affiliation with British Armed Forces or the UK Government within the context of the conflict in Afghanistan.[118]

117. The MOD has acknowledged the gravity of the incidents and the implications of mishandling this type of data relating to 265 vulnerable

[117] MOD Representations, paragraphs 106 to 111.
[118] See paragraph 22.

individuals seeking relocation from a conflict zone. The incidents could have resulted in a threat to life for the affected data subjects, their relatives or associates if intercepted by outside individuals, particularly the Taliban. Short of a risk to life, the data subjects and their known relatives or associates could have also been subject to the risk of torture, harassment or death threats among other acts of targeted coercion. These risks were particularly acute in relation to the 55 affected email addresses that had thumbnails photographs attached, which increased the identifiability of the relevant data subjects.[119]

118. Further, the MOD has also acknowledged the risks of mishandling this data for ARAP itself. In its internal investigation report, the MOD confirmed that if either the Taliban or criminal organisations gained access to any of the data then it could almost certainly be exploited to target ARAP.[120]

119. In addition to the gravity of the potentially egregious implications of a specific personal data breach in the context of a specialist operation like Operation PITTING, the MOD did not generally have in place appropriate measures to ensure the security of personal data processed by the ARAP team when using group emails. The MOD did not give sufficient consideration to the risks involved in the use of group email as a means to communicate with the individuals affected, particularly because communication of this nature had previously been primarily done over the telephone, face-to-face or by one-to-one email. Although a DPIA had been carried out, it was out of date and the risks involved with the switch to using email to contact large groups of eligible persons were not fully considered, recognised or managed.[121] The technical and organisational

[119] MOD Data breach report, dated 21 September 2021, p. 3.
[120] MOD, 'ARAP Internal Incident Report (Partial) for release to ICO', p. 1.
[121] See paragraph 46.

measures in place were therefore not amended to ensure that they were appropriate to the risks involved, even though the MOD could have taken action quickly, as it did after the 20 September Incident.

120. In particular, the MOD did not have a specific policy for bulk communications to external recipients within its JSP 441 guidance, which in fact provided the opposite guidance to what was needed by the ARAP team by discouraging the use of BCC without providing an alternative means of sending group emails securely. Nor were there specific policies for the ARAP team to apply in the course of sensitive and high-risk operations such as Operation PITTING in order to safeguard the personal data of vulnerable individuals. Members of the ARAP team therefore used BCC on an ad-hoc basis, without written guidance on the appropriate use of BCC or access to more suitable software that would allow emails to be sent to multiple recipients individually. This oversight by the MOD exposed the ARAP team's operations to a high degree of risk of human error, which was compounded by the pressurised environment that these communications were being handled within.

121. The MOD submitted that the Commissioner must have regard to the urgent and intense environment in which the data incidents occurred. As explained throughout this notice, the Commissioner has taken the undoubtedly pressurised circumstances in which the ARAP team was operating into account, including in assessing the nature and gravity of the infringement. Having regard to those circumstances, and taking into account the seriousness of the infringement, the Commissioner remains of the view that a fine is appropriate in this case.[122]

122. In terms of duration, the 20 September Incident itself was addressed promptly after it had been identified. The MOD submitted that any

[122] This point is also addressed in paragraphs 136 and 137 below.

infringement should only be considered to have started from the end of Operation PITTING to the reporting of the 20 September Incident on 21 September 2021 and therefore considers that the Commissioner should take into account the fact that the duration of the incidents was very brief.[123] However, the infringement is not confined to the incidents that took place in September 2021 because the Commissioner's concerns also relate to the MOD's broader failures regarding the technical and organisational measures in place for the ARAP team, including the lack of guidance in JSP 441. This period lasted from at least 13 August 2021 to 21 September 2021.[124]

(b) the intentional or negligent character of the infringement

123. The Commissioner does not consider that the MOD acted intentionally in committing the infringement. The Commissioner does, however, find that the MOD was negligent (within the meaning of Article 83(2)(b) UK GDPR) in failing to maintain an appropriate level of security of personal data in the light of the security risks involved with the MOD's processing activities in relation to ARAP. As noted above, the MOD submitted that the Commissioner should not issue a fine because "*the incidents were not wilful, deliberate or negligent: they were the result of human error and an intense and urgent environment*".[125] The Commissioner agrees that the infringement was not committed wilfully or intentionally. However, he remains of the view that the MOD was negligent for the reasons set out below.

124. In that regard, the Article 29 Working Party guidelines (as adopted by the European Data Protection Board) on the application of administrative

[123] MOD Representations, paragraph 111(c).
[124] See paragraph 68.
[125] MOD Representations, paragraph 110.

fines, state that "*failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner and failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence*".[126]

125. Given its size, stature and experience, the MOD ought to have been well aware of the risks involved with mishandling data during specialist and urgent operations. It ought to have been especially vigilant given the heightened risks of data breaches or cybersecurity incidents putting the lives of individuals seeking relocation from Afghanistan at risk. At the very least, it ought to have taken reasonable steps to prevent avoidable data breaches caused by human error, including by not relying on the use of BCC when communicating with multiple recipients by email. In that regard, the MOD should have considered the use of alternative software solutions for sending individual emails, instead of manual reliance on using BCC. Having taken the decision to use Microsoft Outlook in the anticipation that only one-to-one emails would be sent to individuals, the MOD should at least have taken steps to mitigate the risks of relying on BCC once group emails began to be used to contact large groups of eligible persons during Operation PITTING and after. This is particularly relevant when the MOD's deputy DPO had rightly identified the need to focus on security measures to protect the personal data processed by the ARAP team, including ensuring any sharing of information was done securely.[127]

[126] Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, dated 3 October 2017, p. 12
[127] MOD Letter to ICO, 16 December 2022, Annex 1.

(c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects

126. The MOD contacted recipients affected by the 20 September Incident within around 40 minutes and requested that they delete their copy of the email, with advice being given to them as to further steps which could be taken to mitigate the situation.[128] However, two of the recipients of the email responded to the entire distribution list. One recipient responded with sensitive information, making their location known to all recipients.[129]

127. The MOD conducted a prompt internal investigation of the 20 September Incident, and has since implemented organisational and technical changes to address the security risks.[130] The MOD has also implemented a range of other improvements to its data protection training and procedures since the 20 September Incident.[131]

(d) the degree of responsibility of the controller or processor

128. The Commissioner has found that the MOD failed in its obligations under Article 5(1)(f) UK GDPR to process personal data in a manner that ensured appropriate security of personal data, having regard to its responsibility, as a controller, under Article 5(2) and Article 24 UK GDPR.

129. In that regard, the Commissioner considers that the MOD was responsible for implementing security measures to protect the personal data and ensure appropriate technical and organisational measures were

[128] The original email in the 20 September Incident was sent at 17.44 on 20 September 2021. The follow up email alerting recipients to the fact that their email addresses may have been compromised was sent at 18:23 on 20 September 2021.
[129] MOD Personal data breach report, 21 September 2021, p. 3.
[130] See paragraph 42.
[131] MOD Representations, paragraph 69.

in place, taking account the nature of the processing and the risks involved. The steps that the MOD took as the data controller were not commensurate to its size and resources or to the seriousness of the risks of the personal data of the individuals seeking relocation from Afghanistan being compromised.

(e) any relevant previous infringements

130. There are no relevant previous infringements that the Commissioner is aware of.

(f) the degree of cooperation with the Commissioner

131. The MOD has fully cooperated with the Commissioner during this investigation and has provided evidence on request. In doing so, the Commissioner's view is that the MOD has demonstrated good cooperation, albeit that would be reasonably expected of any public authority.

(g) the categories of personal data affected

132. The personal data affected by the infringement of Article 5(1)(f) UK GDPR is described above in paragraphs 53 - 61. The MOD acknowledged during the investigation that "*the information that was shared could result in threat to life".*[132] In its Representations, the MOD revised its position, somewhat downplaying the risks resulting from the disclosures on the basis that the email addresses disclosed "*were unlikely in most cases to contain the data subjects' name or identifying features or any special category data*".[133] For the reasons set out in paragraphs 62 - 64

[132] Personal data breach, dated 21 September 2021, p.4.
[133] See paragraphs 59 to 61 above and MOD Representations, paragraph 111(d).

above, the Commissioner remains of the view that the nature of the personal data was particularly sensitive and required careful handling.

(h) the manner in which the infringement became known to the Commissioner

133. The MOD notified the Commissioner of the 20 September Incident the day after it occurred, and in any event within the statutory timeframe. The 13 September Incident was similarly reported to the Commissioner on 24 September 2021, after being internally detected on 21 September 2021. In contrast, the 7 September Incident was not identified as part of the MOD's internal investigation, and was not reported to the Commissioner until 19 October 2021.[134]

(i) Compliance with any measures referred to in Article 58(2) previously ordered against the controller or processor

134. There are no applicable measures referred to in Article 58(2) UK GDPR.

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

135. There are no applicable codes of conduct or approved certification mechanisms.

(k) any other applicable aggravating or mitigating factors

136. At the time of the 20 September Incident, the ARAP team was responding to an urgent and time-pressured political situation in

[134] See paragraph 32.

Afghanistan in the aftermath of the decision to withdraw military personnel from the region. The ARAP team was tasked with the core objectives of relocation and assistance for at-risk Afghans seeking relocation. The MOD explained that staff were receiving hundreds of emails a day from at-risk Afghans, with members of the ARAP team working long shifts around the clock to identify eligible cases and to establish contact.[135]

137. The Commissioner recognises that, as a result of this combination of urgency and the volume of workload, the ARAP team faced a very significant challenge and was in a difficult situation – with additional personnel joining the team at short notice to augment resources. However, while the specific circumstances of the urgent withdrawal from Afghanistan may not have been foreseen, for the reasons set out in this notice the Commissioner considers that the MOD ought to have had appropriate systems and processes in place to ensure the security of group email communications with individuals supporting the UK's military efforts in conflict zones.

138. The MOD submitted that the Commissioner should take into account the fact that the MOD has committed to establishing a compensation scheme to directly compensate those affected by the data incidents. In the MOD's view such a scheme is more effective than any fine imposed by the Commissioner and a better use of public funds. The Commissioner very much welcomes the MOD's commitment to provide a compensation scheme for those individuals affected by this incident. However, he considers that such a compensation scheme is complementary to an administrative fine imposed by the Commissioner, given the latter is aimed a different purpose, namely to ensure compliance with data

[135] MOD Letter to ICO, 16 December 2022, paragraph 19.

protection legislation, provide an appropriate sanction for the infringement, and act as an effective deterrent against future infringements. This purpose is to be distinguished from the right to compensation for individuals who have suffered damage.[136]

C. Conclusion on whether to impose a penalty

139. For the reasons set out above, and in accordance with the Commissioner's Regulatory Action Policy[137], the Commissioner has decided to impose a financial penalty on the MOD. In reaching this decision that a financial penalty would be appropriate, the Commissioner has, in particular, taken into account the seriousness of the infringement, including the number of individuals that were affected and the degree of potential damage or harm, especially as a result of the risk to life arising from the incidents.

140. In June 2022, the Commissioner set out a revised approach to public sector enforcement to be trialled over two years.[138] To support this approach, the Commissioner committed to working proactively with senior leaders in the public sector to encourage compliance, prevent harms before they occur, and learn lessons when things have gone wrong. In practice, this means that for the public sector the Commissioner has committed to increasing the use of public reprimands and enforcement notices, only issuing fines in the most egregious cases.[139]

[136] See Article 82 UK GDPR.
[137] ICO, Regulatory Action Policy, November 2018 (Available here: Regulatory Action Policy (ico.org.uk)).
[138] Open letter from UK Information Commissioner John Edwards to public authorities, 30 June 2022.
[139] See ICO25 – Our Regulatory Approach, 7 November 2022, p.7.

141. The Commissioner has had regard to the revised public sector approach in reaching the decision to impose a penalty in this case. The MOD submitted that a fine is unsuitable because it would be disproportionate and it would be more appropriate in the present case to issue a reprimand.[140] However, for the reasons set out in this notice, the Commissioner is satisfied that this case is one which meets the criteria for formal enforcement action, and indeed is sufficiently egregious to warrant the imposition of a monetary penalty to reflect the seriousness of the infringement and the significant risk to data subjects, including the risk to life. Accordingly, the Commissioner is also satisfied that imposing a penalty in this case is effective, proportionate and dissuasive and in line with the Regulatory Action Policy.

VI. CALCULATION OF THE PENALTY

142. The process the Commissioner follows in deciding the appropriate amount of penalty to be imposed in an individual case is described in the Regulatory Action Policy, which sets out a five-step penalty-setting mechanism:

a. Step 1. An 'initial element' removing any financial gain from the breach.
b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.
c. Step 3. Adding in an element to reflect any aggravating factors.
d. Step 4. Adding in an amount for deterrent effect to others.

[140] MOD Representations, paragraphs 106 and 112.

e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).[141]

A. Step 1: An 'initial element' removing any financial gain

143. The MOD did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the infringement. The Commissioner has not, therefore, included an initial element at this stage.

B. Step 2: Scale and severity

144. In determining the appropriate element to censure the infringement based on its scale and severity, the Commissioner has had regard, so far as relevant, to the matters listed in Articles 83(1) and (2) UK GDPR.

145. *Nature, gravity and duration*: For the reasons set out in paragraphs 116 - 122 above, the Commissioner is satisfied that taking into account nature, gravity and duration the infringement was serious. Accordingly, the Commissioner has decided that a figure of £1,000,000 is appropriate to reflect the nature, gravity and duration of the infringement. The Commissioner has, in particular, given weight to the following factors in reaching this decision:

a. Although there is no evidence of actual harm being suffered, there was a high risk of potential harm to the affected data subjects or their family members. As recognised by the MOD, this potential harm included a serious threat to life as the individuals affected were in a vulnerable position seeking

[141] Regulatory Action Policy, p.27.

relocation from Afghanistan and, if the information fell into the wrong hands, it could almost certainly be exploited to target ARAP. Further, it is likely that distress was caused to the affected data subjects and their relatives after being notified of their compromised email addresses, compounding the seriousness of the infringement. The Commissioner has taken into account the MOD's submissions that the Commissioner has overstated the likely or potential impact of the incidents, but remains of the view that the personal data involved was sensitive and required careful handling.

b. The Commissioner considers that the most egregious aspects of the infringement involved the risk of harm, or potential harm, caused by the actual personal data breaches in September 2021. However, the MOD was also responsible for failings in respect of the technical and organisational measures it should have had in place for the ARAP team to ensure the security of sending group emails to large groups of eligible persons in Afghanistan. The Commissioner considers that these failings directly contributed to the incidents in September 2021, given that the reliance on BCC and lack of adequate measures in place to mitigate the risks of inadvertent disclosure exposed the ARAP team to a heightened risk of human error, and this is reflected in the size of the penalty.

c. The Commissioner also considers that the infringement was of greater seriousness because it was not simply a "one off" event, but a failure attributable to the deficiencies in the technical and organisational measures that the MOD had in place to ensure the security of personal data processed by the ARAP team. These

deficiencies lasted from at least 13 August 2021 to 21 September 2021 (see paragraph 67).

146. *Intentional or negligent character of the infringement*: As set out in paragraphs 123 - 125, the Commissioner considers that the infringement was not intentional. No uplift has therefore been made on that basis.

147. *Action taken by the controller to mitigate the damage suffered*: As set out in paragraphs 126 - 127, the Commissioner considers that there were limited containment and remedial actions that the MOD could have taken after the 20 September Incident occurred. This was because once the information had been disclosed, there were limits as to how it could then be retrieved, protected and controlled. However, the Commissioner acknowledges the swift action taken by the MOD to contact the individuals affected by the 20 September Incident to advise them of the steps to take to protect themselves, as well as the remedial actions and organisational change that the MOD took following the 20 September Incident. Taking into account the action taken, the Commissioner considers that it is appropriate to reduce the penalty amount by £100,000.

148. *Degree of responsibility of the controller*: As set out in paragraphs 128 - 129, the Commissioner's view is that the MOD should have recognised the risks involved and taken the necessary appropriate steps to ensure the personal data of the individuals seeking relocation from Afghanistan was kept secure. Although the MOD advised that it could not foresee the political turmoil it would be working in following Operation PITTING, the Commissioner considers that the very nature of the ARAP team's activities should have prompted the MOD to implement suitable measures to reduce the risks of a personal data breach, rather than relying on the BCC field within Outlook, or at least taken steps to mitigate

the risks of relying on BCC once group emails began to be used to contact large groups of eligible persons during Operation PITTING and after. However, the Commissioner has decided that, given the nature of the infringement, the responsibility of the MOD to put in place appropriate technical and organisational measures has already been taken into account in the amount of penalty imposed to reflect the nature, gravity and duration of the infringement. The Commissioner therefore does not consider it is necessary to change the penalty on this basis.

149. *Degree of cooperation with the Commissioner*: As set out in paragraph 131, the MOD has demonstrated an appropriate level of cooperation and the Commissioner does not propose to change the penalty on this basis.

150. *The categories of personal data affected*: As set out in paragraph 132, the Commissioner considers that the data involved was particularly sensitive and required careful handling. However, the Commissioner does not propose to change the penalty on this basis as the data affected has already been properly taken into account when considering the nature and gravity of the infringement earlier in Step 2 of the penalty calculation.

151. *The manner in which the infringement became known*: As set out in paragraph 133, the MOD reported the 20 September Incident to the Commissioner the day after it occurred. It similarly then reported the 7 September Incident and 13 September Incident when these were identified following further internal investigation. Although, the Commissioner would have expected the MOD to have identified the two earlier incidents sooner, the Commissioner does not propose to change the penalty on this basis as the failings relating to the MOD's internal process have already been properly reflected when considering the

nature and gravity of the infringement earlier in Step 2 of the penalty calculation.

152. *Any other applicable aggravating or mitigating factors*: As set out in paragraphs 136 - 138, the Commissioner recognises the very significant challenges that the ARAP team faced and the urgent and pressurised circumstances of the evacuation from Afghanistan. For the reasons given in this notice, the Commissioner does not consider that these factors, or the fact that the MOD was not playing its typical role in this type of operation as envisaged by JDP 3-51, mean that the infringement found was not sufficiently serious to warrant the imposition of a fine. However, the Commissioner has decided to reduce the penalty by £200,000 to take into account the challenges the ARAP team faced and the urgent and pressurised circumstances it was working in.

153. Accordingly, the penalty following the application of the factors in Article 83(2) is £700,000.

154. As required by Article 83(1), the Commissioner has considered whether the penalty of £700,000 at Step 2 would be effective, proportionate and dissuasive.

155. The Commissioner has decided that it would be, taking into account the following points:

    a. Infringements of Article 5(1)(f) are subject to the "higher maximum amount" of administrative fines under Article 83(5) UK GDPR, i.e. up to £17.5 million or, in the case of an undertaking, 4% of total worldwide annual turnover (whichever is higher).

b. As a government department, which is not an undertaking and which has no annual turnover, the maximum penalty amount for a contravention of Article 5(1)(f) UK GDPR would be £17.5 million. An amount of £700,000 is well below this maximum amount.

c. The infringement was of a sufficiently serious nature to warrant a significant penalty, given the fact that lives were put at risk. While penalties are assessed on a case by case basis and the Commissioner is not bound by previous decisions, by way of comparison the penalty imposed for failures relating to the use of BCC by an NHS hospital trust could have been up to £784,400 (the penalty was reduced to £78,400 in that case under the Commissioner's revised approach to public sector enforcement).[142]

d. Similarly, under the previous data protection legislation, the Data Protection Act 1998, the Commissioner imposed penalties for breaches relating to the inadvertent use of the "To" or CC fields instead of the BCC field.[143] Other cases involving security breaches have also resulted in large fines under the DPA, including those relating to Interserve, British Airways and Marriott, demonstrating the importance of compliance with Article 5(1)(f) UK GDPR.[144]

---

[142] Tavistock & Portman NHS Foundation Trust, Monetary Penalty Notice, 9 June 2022, paragraph 53. In addition, a reprimand (rather than a penalty) was imposed on another NHS trust, NHS Highland, on 9 March 2023 for inadvertently using CC rather than BCC when emailing 37 individuals likely to be accessing HIV services. The Commissioner notes that the infringement by NHS Highland involved fewer data subjects than were affected in the present case and, while serious, the disclosures in both cases did not involve putting lives at risk in a conflict zone.
[143] For example, the Information Commissioner fined the Independent Inquiry into Child Sexual Abuse £200,000 in a decision dated 5 July 2018 in respect of a BCC security breach. The Commissioner had previously issued monetary penalty notices for similar breaches to Bloomsbury Patients Network (11 December 2015) and Chelsea & Westminster Hospital NHS Trust (4 May 2016).
[144] See: Interserve, Monetary Penalty Notice, 19 October 2022; British Airways, Monetary Penalty Notice, 16 October 2020; and Marriott International, Monetary Penalty Notice, 30 October 2020.

e. Imposing a penalty in this case will have a genuine deterrent effect, discouraging both the MOD and others from committing a similar type of infringement in the future. While the MOD has already taken measures to improve its processes, imposing a penalty in this case will also help ensure that other controllers comply with the requirements of UK GDPR by implementing effective technical and organisational measures, in particular by improving the understanding the risks to security of relying on BCC when sending emails to multiple recipients.[145]

156. Accordingly, for the reasons set out above, the Commissioner's conclusion at Step 2 is that a financial penalty of £700,000 is appropriate to reflect the seriousness of the breach, taking into account the need for the penalty to be effective, proportionate and dissuasive.

C. Step 3: Adding in an element to reflect any aggravating factors not accounted for above (Article 83(2)(k))

157. The Commissioner has not identified any aggravating factors, beyond those considered above, which would warrant further increasing the penalty.

[145] In its Representations (at Paragraphs 107 - 108) the MOD has suggested that it is not necessary to dissuade the MOD, noting that it has "*unarguably learnt from this incident*", as demonstrated by the changes made to address the areas of concern. The MOD also suggested that a fine was not necessary to deter others given the "*highly unusual circumstances of this case*". However, for the reasons explained at paragraph 155(e) of this Penalty Notice, the Commissioner considers that the risks around the use of BCC are risks which extend beyond the specific circumstances of this particular infringement. The Commissioner has also already taken into account the urgent and pressurised environment in which the ARAP team was operating as a mitigating factor to reduce the amount of the penalty.

D. Step 4: Adding an amount for deterrent effect to others

158. The Commissioner is under an obligation to impose a penalty which is "dissuasive". The need for the penalty to be dissuasive in relation to the MOD itself is addressed by the analysis at Step 2. Having regard to the amount of the penalty identified under Step 2, the Commissioner does not consider it necessary to increase the penalty further under Step 4 to dissuade others. The Commissioner therefore considers that no adjustment is necessary under Step 4.

E. Step 5: Reducing the amount to reflect any mitigating factors not accounted for above, including ability to pay

159. The Commissioner has not identified any mitigating factors, beyond those considered above, which would warrant decreasing the penalty.

F. The Commissioner's approach to public sector enforcement

160. As explained in paragraphs 140 - 141, although the Commissioner set out in June 2022 a revised approach to public sector enforcement, in this case the Commissioner has decided that a monetary penalty of £700,000 should be imposed. However, taking into account the fact the MOD is a government department and therefore a public body, the Commissioner has decided that it is appropriate to reduce the amount of the penalty by 50% to £350,000.[146]

[146] In its Representations, the MOD drew reference to the Commissioner's decision in Tavistock & Portman NHS Foundation Trust, Monetary Penalty Notice, 9 June 2022 in which a 90% reduction was applied, and submitted that it was unclear why a lesser reduction has been applied to the MOD. The Commissioner is not bound by previous decisions, which of course turn on their own merits and circumstances, and in this instance a reduction of 50% is considered proportionate, particularly when taking into account the risk to life.

G. Conclusion - Penalty

161. For the reasons set out above, the Commissioner has decided to impose an administrative penalty on the MOD in the amount of £350,000.

VII. PAYMENT OF THE PENALTY

162. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **11 January 2024** at the latest.

163. The penalty is recoverable by Order of the County Court or the High Court.

164. Commissioner will not take action to enforce a penalty unless:

- the period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

VIII. APPEAL

165. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

- the imposition of the penalty; and/or

- the amount of the penalty specified in the Penalty Notice.

166. Any notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice.

167. Your attention is drawn to Annex 1 to this Penalty Notice, which sets out details of your rights of appeal under section 162 DPA.

Dated: The 7th day of December 2023

[redacted]

John Edwards, Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

Rights of appeal against decisions of the Commissioner

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   General Regulatory Chamber
   HM Courts & Tribunals Service
   PO Box 9300
   Leicester
   LE1 8DJ

Email: grc@justice.gov.uk
Telephone: 0300 123 4504

a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the Penalty Notice.

b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal 30 Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).