No.	Near miss / breach (risk rating)	Date of awareness	Description of breach/near miss	Cause	Action item(s)	Follow up needed	Follow up category	Notification(s) Required? Risk assessment and rational for decision.	NPES	Close out date for follow up	Revelant Docs Location
1	Breach (No risk)	15/03/2019	Error with Prism including stakeholder's name in the "to" field of certain emails send from Prism to service providers. Although the email is in fact going to service provider, it appears as if it going to the stakeholder named in the email instead and looks as if HIQA sent the email to the incorrect person.	Minor system error with Prism. Occurs where the service provider email is a generic one and the system defaults to use an associated stakeholder name instead of the generic email address.	DPO to follow up with relevent personnel and IT to fix issue.	Yes.	Resolve IT issue	No. Deemed not to pose a risk to the rights and freedoms of natural persons as disclouse to trusted reciepent and data limited to the name of individual which was already know to the the service provider. As such notification to DPC not required under Article 33 GDPR	N/A	End April	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB01_2019
2	Breach (High Risk)	28/03/2019	Inspection report published online containing information about an employee at the centre; information related to their performance in the role. While not named, the employee was idenfiable based on the details provided and limited number of staff.	Centre provided this information in responding to the compliance plan. It was noted that centre provided info and centre asked to provided a clean version of comments for report. Human error resulted in old report being uploaded rahter than clean copy.	Report removed from website inmediately. Meeting between DPO and RMs to review. Breach cannot reoccur due to process change implemented shortly after report published. Other reports checked and it was verified that error did not recoccur.	Yes.	Process review, change implemented shortly after publishing report means error cannot reoccur.	Yes. High risk due to the content of information which discussed employee's personal matters. Notification made to DPC (rating high risk) and DS, as required by Articles 33 and 34.	N/A	End April	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB02_2019
3	Breach (No Risk)	29/04/2019	Notification email sent from PRISM to incorrect designated centre. Only personal data in the notification was the HIQA inspector's contact details at the bottom of the email.	Human error	DPO spoke to person reporting incident, who explained that email notification was sent to the wrong center and gave detailed description of the content of the email. DPO conducted risk assessment. Once off human error	No	NA	No. They only personal data that was contained in the notification was the name of the HIQA inspector who sent notification. The recipient was a designated centre regulated by HIQA. Recipient confirmed deletion of the email. Due to the relationship between HIQA and the recipient, the incident is a disclosure to a trusted recipient, whose statement that the data has been deleted can relied upon. Due to the above circumstances, there is no risks to the rights and freedoms of the data subject, i.e. the HIQA employee whose contact details were contained in the bottom of the notification.	N/A	N/A	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB03_2019
4	Breach (Low Risk)	09/05/2019	Payslip sent by data processor to wrong recipient. Payslip returned by the recipient, who was a former employee with a similar name.	Error by Processor	DPO spoke to person reporting incident, and contacted recipient to confirm that they only received the one payslip and no copies made. Conducted risk assessment of breach, and contacted data processor. Data processor conducted investigation and confirm cause was technical glitch.	Yes.	Asked processor for expaination and advise of measures implement to address risk.	Yes. Risk assessed to pose a low risk to rights of the data subject; although payslip returned another person did had sight of it and has potetntial to impact rights of data subject. Notification made to DPC (rating low risk). Letter also sent to the DS to infrom them of incident and advise of steps taken. Report requested from processor and provided.	N/A	N/A	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB04%202019
5	Breach (No risk)	29/05/2019	Email sent to wrong DC containg name of PIC, no other personal data. Recipient another DC, which informed HIQA of receiving email in error. Reported by NS, updated report provided by DL subsequently with furhter detail.	Email address entered incorrectly	Recipient requested to delete email and confirm deletion, provided on 29/05/2019.	No	NA	No. Risk assessed to be no risk due the limited personal data concerned, name of PIC, which is publically available. No other content in email related to to PIC. Email recipient was a trusted recipient who deleted email and cofirmed the same	N/A	30/05/2019	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB05%202019

6	Breach (No Risk)	14/06/2019	Email sent to incorrect service provider. An inspector was cc'd on email to centre, however, the email that was used for the inspect was a previous email address that was listed under the inspector, who was formerly an employee of a service provider, being used and sent to the inspectors former employer. Updated breach report provided by DL subsequently.	Human error	DPO spoke with regional manger who made report. Service provider who received email contacted and asked to delete the email and confirm deletion which they did. Inspector's details on PRISM reviewed and stakeholder ID deleted to prevent reoccurance.	No	NA	No. Risk assessed to be no risk due the limited personal data concerned, name of PIC for a centre, which is publically available, and HIQA employee details. Email recipient was a trusted recipient who deleted email and cofirmed the same	N/A	20/06/2019	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB06%202019
7	Near Miss	20/06/2019	Error in filing in registration files resulted in documents being misplaced and unattainable when required. Reported by LV.	Human error	DPO spoke to archivist and need to return files from off site and redo filling. Archivist suggested using this as a training exercise	No	Training	Not a breach; near miss.	N/A	TBC	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB07%202019
8	Breach (No Risk)	26/06/2019	Following mailmerge on outlook for outstanding registered providers, letters re fees issued to incorrect email addresses.	Human error	DPO spoke to team. Immediate action taken to stop mail merge and reciepients who were sent emails cotnacted to confirm deletion which they did.	No	NA	No. DPO reviewed the letters that issued in error and confirmed that the only personal data contained within them is the name and title of Bob Hennessey, Deputy Director of Regulation. No personal data relating to members of the public or service providers appear in the letters. In addition, the recipients can be deemed to be "trusted recipients" who can be relied upon to follow the instruction to delete the email received. Accordingly, risk assessed the breach as "no risk" or a breach that does not pose a risk to the rights and freedoms of data subjects.	N/A	27/06/2019	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB08%202019
9	Near Miss	28/06/2019	Email sent to @hiqa address meant for another recipient. Recipient was an external person. However, address was created to register user of decision time app so wasn't live email that could receive mail. So no email received.	Human error	DPO issued with person reporting incident, reviewed email and circumstances.	No	NA	No. Email was not live so recipient could not receive email so no breach in this instance.	N/A	28/06/2019	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB09%202019
10	Near Miss	12/07/2019	HSE rep sent in an access request for Portal for a number of Centres that she was associated with, including one which was a private nursing home and to which she was not entitled to have accesss to. She was given access to all of the OSV s on the 25th of January. The incident had potential to give rise to "unauthorised access" to personal data held on OSV file, however, the account for the private nursing home was not accessed. This is evidenced by the portal log details.	Human error	Team member DPO to discuss and submitted breach report on 15/7/2019. Reviewed by DPO.	Yes; change to process needed to double check requests from HSE are only for centres under their remit.	Process change	No. Not a breach as the information was accessed or disclosed in this instance, however, if circumstances had been different and the account was accessed it would have been a breach.	N/A	17/07/2019	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB10%202019
11	Near Miss	16/08/2019	Email accidently sent to wrong recipient; a family member of the sender with similar name. Sender spotted error once email sent and then access the account of family member and deleted the email. No one other than sender had access to the email.	Human error	CG reported to DPO on 16/08/2019 and DPO followed up in 19/08/2019 (on leave previously). DPO issued incident and reviewed report	No; one off human error	NA	No. No personal data was contained in the email so not a breach. Also email was deleted by sender without anyone accessing the email or no authoirised access etc. Incident logged as near miss.	N/A	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB11%202019

12	Breach (No risk)	12/08/2019	Email containing internal correspondence and attached invoice in respect of payment of legal advices sent to the wrong recipient. The person who received the email in error had a very similar name to the intended recipient and the sender put this name by mistake. The person who received the email contacted the sender to say they received the email and to confirm deletion. Reciepient, an emloyee of ATOS, is a service provider of HIQA s.	Human error	LK reported to DPO on 12/08/2019 and DPO reviewed content of email sent. Risk assessed as no risk breach. Report compiled and forwarded.	No; one off human error	NA	No. Risk assessed as no risk breach. The email was sent to a "trusted recipient" who can be relied upon to have deleted the email upon receipt as they stated and thus mitigate the risks concerned. Also the emails contained little personal data other than professional or work related details, i.e. email addresses, invoice details, etc which can be considered to pose no risk.	N/A		http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB12_2019
13	Breach (Med Risk)	09/09/2019	Unauthorised access of HIQA employee email account via "hack" of webmail platform. Access gained to email account for a number of hours on Sat 7 Sept, and account used to send SPAM type emails to recipients both internal to HIQA and externally. Employee whose account was compromised contacted ICT and on Monday when ICT came on-line immediate action was taken to lock down the account and investigation started. Incident reported to IG manager as DPO on holidays. DPO followed up with ICT lead on return and furhter details discussed as coming to light. based on these DPO made assement that there was a data breach and made report to DPC on 17/08/2019.	External "hack" of webmail platform	ICT immediately locked down account when it became aware of breach on Monday morning and commenced investigation. Password of user changed. DPO became aware of incident on return to work on 16 Spet, and received furhter info on 17 Sept, based on this information which indicated that the email account was hacked from an external party, DPO compiled report to the DPC and issued that evening.	Yes. DPO meeting ICT to review incident response plan. Specific follow actions identifed and agreement reached re achieving these. External consultants, BDO engaged to produce report.	Yes, undertaken.	Yes. It was established that there was unauthorised access to email account, which creates a strong likelihood of loss of confidentiality in respect of the content of the account. The fact that the email account was a work based on reduces risk of impact to professional sphere, however, risk remains. The a single email account was hacked was this also refduces risk. Notification made to DPC (rating medium risk) as required by Articles 33. As risk not deemed to be high risk, there was no requirement to report to the affected data subjects. However, the email account user is aware of the breach and has changed password.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB15%202019
14	Breach (No risk)	18/09/2019	Attendence list from awareness event, including the name and work email of those attending was misplaced. Believed to have been disposed of in secure bin during desk clear out. Document located next day.	Human error	Reported to DPO once member of staff became aware attendance list may have been accidently disposed of.	No.	N/A	No. Breach determined not to pose a risk to rights and freedoms of indivduals due to the nature of the data contained, i.e. names and email addresses, in the sign in sheet and purpose of the sheet, i.e. record of awareness event. Also believed to have disposed of securely in secure shredder bin. Document found the next day in a notebook.	N/A	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB14%202019
16	Breach (No risk)	24/09/2019	Annotification letter was issued to the incorrect provider. Once the error was discovered, the correct letter was issued to the provider with an apology for any inconvenience caused. It was alerted to the DDOR, to the DPO and the Provider that recieved letter was sent an email asking them to confirm deletion. The letter contained limited personal data i.e. names of two people working at the centre and details of the steps needed to complete their notifications to HIQA.	Human error	DPO reviewed notification letter that issued and confirmed only personal data was name of two employees working in centre; advised emailing person who received email in error to ask for deletion and confirmation of the same. This was done and confirmed.	No	NA	No. DPO Assessed that breach poses "no risk" to individuals considering the limited information in the letter; names of two employees and actions to be taken to complete the notification. No other identifiable informaiton present. Incorrect recipient is regualted by HIQA and so a "trusted recipient" that can be relied upon HIQA's instruction to delete email.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB16%202019/Data%20Breach%20Reporting%20-%20DB%2016%202019.docx

17	Near Miss	23/09/2019	Notice of Proposed Decision was sent to the provider, this email was sent through PRISM; however it was also copied to the inspector EC, however, instead of adding the user EC to the email, the stakeholder EC was added to the email. This stakeholder was not a stakeholder in the centre where the Notice of Proposed Decision was being sent. Attempt was made to contact the recipient who recieved email in error, but no response. A bounce back email was later received to initial email stating that this email address is no longer in use. There was no personal data included in this document, only personal data potentially disclosed was email of EC the stakeholder	Human error	Incident reported immediately to the Deputy Director of Regulation and DPO. Attempt made to contact the stakeholder EC, however the number we have on Prism was not in service. email sent to confirm deletion of the document. However bounce back email recieved to this and intial email; neither were recieved by EC.	No	NA	No, not a breach as no personal data disclosed; email that issued was "bounced back" without anyone viewing/accessing contents	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB17%202019
18	Breach (No risk)	26/09/2019	Email sent to the wrong recipient. Email addresssed to two people, one of which was a contact at "St Johns Hospital". However, the contact that the email was sent to was the incorect St John's Hospital (there are a number of these). Contact who received the email in error informed HIQA and confirmed deletion of email. Only personal data disclosed was the email address of the other recipient, a HSE employee. No personal data contained in the email	Human error	Contact who received the email in error has confirmed deletion of email. Sender of email informed DPO, who assessed incident and content of email .	N/A	NA	No. The only personal data that was disclosed was the work email of a HSE employee, which is publically availble online. Information is not confidential and not likely to pose an impact in terms of the rights of individuals. Recipient is a trusted recipient, that can be relied upon to act on instructions of HIQA to delete email. Consequently, the breach is categorised as a "no risk" breach.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB18_2019
19	Near miss	23/09/2019	There was a malfunction within Integra invoicing application on The system experienced an intermittent workflow disruption. This resulted in the system attaching the wrong invoice to the billing email for 19 out of 582 emails going out to registered providers.	System error in Integra	Finance team contacted Integra developers to seek explaination for cause of malfunction. BH informed in regulation. GH in finance reviewed recipients and content of attachements sent in error. Reipents contacted and asked to delete emails. 2 attachments related to NF60s, and these centres were contacted as the info disclosed could be commercially sensitive.	Yes	Resolve Intergra issue	No, content of emails did not contain personal data. Info was business info and did not contain any names etc. However, as the issue which gave rise to the disclosure could have resulted in a breach and invloved the disclosure of commercially senstivie info in 2 cases (NF60s), a number of actions were taken. Finance contacted Integra and a "fix" or update to system was installed. DH also contacted the reicipents who recieveed emails in error. EMT were informed of the issue. DPO and integra suppliers discussed issue of reporting and data protection.	NA	End October	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB19%202019
20	Breach (No risk)	22/10/2019	Email sent to all DCOP and DCD registered providers and PIC s. Email address in the cc slot instead of the bcc slot in error.	Human error	DPO discussed with business area; email issued to recipients asking them to delete email and confirm deletion, email reissued using bcc function	No	No	No. This breach involves a risk of the loss of confidentiality of information relating to the contact details and identify of PICs in the relevant centres. However, given the fact that the information disclosed, i.e. that a particular person works at a centre, is already publically available on the HIQA website under the “find a centre” tabs, which HIQA makes public pursuant to its statutory mandate, I do not think that the disclosure of the information in this instance poses a risk to the rights of individuals concerned. all the recipients to whom the email was sent are “trusted recipients” who can be relied upon to act upon HIQA s instruction to delete the email they received in error. This due to the pre-existing relationship between them and HIQA.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB20%202019

21	Breach (No risk)	13/12/2019	Email with attachment containing A Notice of Proposed Decision was issued to the incorrect provider. The provider who received the Notice has confirmed that they have shredded the document and the the correct provider has advise them of this issue and another NOPD would be issued to them in due course.	Human error	DPO discussed with business area; info disclosed confirmed to be destroyed by recipient and notice reissued to correct recipient.	No	No	No. Risk assessed as no risk breach. The letter was sent to a "trusted recipient" who can be relied upon to have deleted the letter upon receipt as they stated and thus mitigate the risks concerned.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB21%202019
22	Breach (No risk)	19/11/2019	Email sent to incorrect recipient. Disclosure of email addresses of other recipients, no personal data contained in the email body or attached report.	Human error	DPO discussed incident with SM and reviewed report for personal data; none identified	No	No	No. Risk assessed as no risk breach. The letter was sent to a "trusted recipient" who can be relied upon to have deleted the letter upon receipt as they stated and thus mitigate the risks concerned.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB22%202019
23	Breach (No risk)	08/11/2019	Email to provider cc'd in error to person in HSE insead of intended internal recipient	Human error	DPO discussed incident with person reported breach and reiewed content; only personal data email address of other recipients.	No	No	No. Risk assessed as posing no risks because email address publically available and disclsorue to trusted recipient who confirmed delteion of email.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB23%202019
24	Breach (No risk)	05/11/2019	Email send to incorrect recipient; meant fo internal person and to external person with similar name. Info disclosed are 2 internal emails of HIQA employees, no other personal data	Human error	DPO discussed with person reporting and examined email content	No	No	No. Poses no risk considering limited nature of the info disclosed -two email addresses of employees, and recipient has confirmed deletion.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB24%202019
25	Near Miss	04/12/2019	Email sent to person who no longer works in a designated centre. However, email failed to deliver so no info actually disclosed.	Human error	DPO discused incident and contetn	No	No	No. Not a data breach.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB25%202019
26	Near Miss	16/12/2012	Stage 1 report for a designated centre was incorrectly attached to an email intended to send a stage 2 report to another designate centre.	Human error	DPO reviewed report issued and emails sent	No	No	No. Not a data breach as no personal data disclosed.	NA	NA	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB26%202019
27	Breach (No risk)	19/12/2019	A notice of decision was sent by registered post from glaway office but was not received by the recipient a number of days later. The log in registered post book cannot be linked to the letter sent so the address to which it was sent cant be verified or the status checked.	Human error	DPO discussed with business area the need to review process to record log number of registered post with relevent letters to ensure easy of verifiying	Yes	Process review	No. No risk data breach as only name of inpsector was disclosed and the limited nature of this info and fact that inspectors employment with HIQA in public domain means breach does not pose risk.	NA	End Jan 2020	http://edm/CEO/ExecutiveManagementTeam/IG%20Documents/Data%20Breaches%20Reports%20and%20Investigation%20Forms/2019/DB27%202019