Data Protection compliance monitoring report - 2022

Introduction

This is the annual report on SHR's compliance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA) and other related legislation.

An annual assessment is carried out by the Data Protection Officer (DPO) to monitor and report on SHR's level of compliance with the legislation and to identify recommendations to maintain existing good practice and improve overall compliance levels.

The report covers the period 1 January 2022 – 31 December 2022 and sets out the arrangements SHR has in place to ensure compliance with key provisions within the legislation and activity that has been carried out throughout the year.

Information Commissioner's Office (ICO) registration

The ICO Register confirms that SHR is currently registered (reference number ZA119141) and the date of the next registration is 25 May 2023. The existing registration lists the address as Buchanan House so this should be updated to the SHR's new permanent location following the office move.

Data Protection Officer (DPO)

All public authorities are required to have a DPO with an appropriate level of expertise and experience to advise on data protection obligations and to monitor compliance. SHR has a DPO in place on a shared services basis with Transport Scotland. The DPO holds a BCS GDPR Practitioner Certificate and works full time on Data Protection and information governance.

The shared service arrangement is reviewed annually. At the most recent review it was assessed as working well for both parties and was renewed.

Personal data security breaches

There have been six reported personal data security breaches during the reporting period (two breaches were reported during 2021). None were sufficiently serious to require a report to the ICO due to the low risk nature of the data involved.

Five of these breaches were as a result of simple manual error relating to email where information was sent or copied to the wrong recipient. In each case the personal data involved was low risk and appropriate actions were taken to mitigate any risk, including using the email recall function and contacting the incorrect recipient to ask them to delete. Further reminders were issued about the importance of extra vigilance when sending emails and all staff have been encouraged to disable the auto-populate function on Outlook.

The final breach related to a BI system issue where a small number of contact details of correspondents were temporarily visible to landlord admin users. The personal data involved was low risk and action was taken quickly to fix the issue and disable the functionality that enabled the details to be viewed.

Subject access requests (SARS)

Two requests for access to personal data were received during the reporting year (five requests were received during 2021). The requests were handled by policy areas with input and advice from the DPO and legal advisors where required. The response to both requests were issued within the statutory timescales.

Information Commissioner's Office (ICO) complaints

No complaints were received from the ICO during the reporting period.

Data Protection Impact Assessments (DPIAs)

A DPIA must be carried out to identify and minimise privacy risks for processing personal data where it is likely to result in a high risk to individuals. SHR has an agreed DPIA process which includes initial screening criteria to help determine whether a full DPIA is required. The SHR DPIA template was recently updated to include a section that can be populated to obtain the decision making audit trail when it has been assessed that a full DPIA is not required.

During the reporting period a screening exercise was carried out on the procurement exercise for the delivery of the National Panel of Tenants and Service Users. This was completed by the relevant business area and approved by the DPO. It was assessed that the processing involved was low risk therefore a full DPIA was not required.

Personal data mapping and Information Asset Register (IAR)

It is recommended that the personal data register and IAR continues to be reviewed and updated at least annually. The last full review of these registers was conducted in December 2022 and they are currently up to date.

Data processors and data sharing

It is a requirement under GDPR for a contract with standard GDPR clauses to be in place with all third parties who process personal data on our behalf. The mandatory GDPR clauses are included within all existing contracts and they are put in place as standard for any new contracts.

The on-going work to progress the Data Sharing Agreement between SHR and SG HR Shared Service for the provision of HR and payroll services was superseded by advice from central SG HR that the existing agreements in place were sufficient for GDPR purposes. This view was confirmed by the SG DPA team therefore SHR were content to agree that this activity was complete.

Work on the project to further roll out Objective Connect as a method for secure transfer of information will continue in the next reporting year when new resource is in place to take this activity forward.

Staff training

It is mandatory for all staff to complete the online GDPR e-learning on an annual basis, therefore the training should be routinely communicated to all staff and completion rates monitored every year.

All SHR staff have completed the mandatory training within the required timescales during 2022.

Overall compliance:

SHR has retained a good level of compliance with data protection legislation and it is positive to note there have been no Data Protection related complaints or serious/reportable breaches during the reporting year. However the number of low level manual breaches has increased from last year so all SHR staff have been encouraged to take extra care when using email. The DPO delivered a GDPR refresher session for SHR staff towards the end of the year which included hints and tips about effectively reviewing the contents and recipients of emails prior before issue.

The Information Management Group (IMG) continues to meet regularly to discuss information governance compliance and to identify and implement action for continuous improvement.

The following actions are recommended to sustain and/or improve the existing level of compliance:

Recommendations

- Complete the regular annual review and update of the personal information register and IAR during 2023
- Update the address on the ICO registration to reflect SHR's new location following the permanent office move
- Conduct the regular annual review of the SHR DPO arrangements during the 2023
- IMG to continue to review and update its annual work plan and progress the on-going action around secure transfer of information when new resource is in place
- Continue to reinforce good practice information management and security through regular staff communications and conduct lessons learned exercises following any reported information security breach
- Promote the mandatory GDPR e-learning module to all staff and monitor annual completion rates

Review of activity from 1 January – 31 March

SHR's Data Protection Policy was updated and the revised version published on the website in February 2023. It is next due for review in 2025.

Lorna Clark
Data Protection Officer (DPO)
February 2023