South Ribble Council &
Chorley Council

Final
Internal Audit Report

GDPR Transparency
2023/2024

Audit Assurance: Adequate
Auditor: Linsey Roberts
Date Issued: 15th December 2023

Cert No: 20128

South Ribble Borough Council | Chorley Council

WORKING TOGETHER

	Reason for the Audit & Scope
1	UK organisations that process personal information need to comply with the Data Protection Act 2018/UK General Data Protection Regulations (UK GDPR). Organisations are required to adhere to the seven key principles that lie at the heart of the GDPR regime. Failure to comply with the principles may leave the Council open to substantial fines (up to £17.5 million, or 4% of annual turnover, whichever is higher). This review included the following elements of the first principle 'lawfulness, fairness and transparency': • You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned. • You must be clear, open and honest with people from the start about how you will use their personal data. This is especially important in the following situations, and formed the focus of the review: • individuals have a choice about whether they wish to enter into a relationship with the Council. If individuals know at the outset what their information will be used for, they will be able to make an informed decision; also • when the Council has no direct relationship with the individual and collects their personal data from another source. This review is included in the 2023/24 Annual Audit Plan approved by the Governance Committee on the 7th March (SRBC) and 15th March (CBC) 2023.

	Audit Objectives
2	The overall objective of the audit is to provide an opinion of the adequacy, application and reliability of the key internal controls put in place by management to ensure that the risks listed below are being sufficiently managed. • The data subject is not informed about how their personal data will be used; • The personal data is processed in a way that is detrimental, unexpected or misleading to the individual. Whilst it was originally anticipated that the review would also include evidence of consent, due to the complexity of the differing types of service the Councils are now providing, it was decided that this would warrant a separate review and will be considered for future audit plans. A sample of 10 Chorley Council, 12 South Ribble and 3 shared service areas were reviewed to assess compliance with the requirements set out in guidance supplied by the Information Commissioners Office.
3	The audit also assessed the effectiveness of the various other sources of assurances using the three lines of defence methodology.

	Audit Assurance
4	On an annual basis, a review of a GDPR principle is undertaken, and this was the first time a review considered the transparency aspects of the regulations.
5	The Head of Internal Audit is required to provide the Governance Committee with an annual audit opinion on the effectiveness of the overall control environment operating within the Council and to facilitate this each individual audit is awarded a controls assurance rating. This is based upon the work undertaken during the review and considers the reliance we can place on the other sources of assurance.

6	Our evaluation of the reliance we can place on the three lines of defence is shown in Appendix B.
7	To ensure both Councils comply with UK GDPR and the Data Protection Act, shared data protection policies are in place, up to date and readily available for officers. Mandatory GDPR training is provided to ensure all employees at both Councils understand their responsibilities and our review found that the majority of staff contacted for this review had completed this training. This review focussed on three separate aspects of transparency to ensure that service users are aware that their data is being treated lawfully and for the purpose it is provided. The three aspects were: • Privacy notices; • Point of collection of data and • ROPA details. Our review identified that a significant amount of work has been undertaken at each Council and that a general privacy policy/notice and service specific privacy notices are in place and accessible on the Council's websites. The format of these are consistent with the Information Commissionaire Office (ICO) requirements and the content is clear and transparent demonstrating how personal and sensitive data is handled. However, despite the fact that both Councils are offering similar or same services, there are gaps in the notices which should be addressed to ensure consistency in approach. Data is collated through the Contact Centre / Gateway via telephone contact. Previously an automated data protection message was relayed prior to customer contact however, this is now not in place and customer services staff are not providing a scripted message prior to collecting a customer's personal data. Completion of automated forms via the website or manual paper-based forms is the main form of data collection. It was established that whilst a large proportion of forms or terms and conditions included sections of data protection legislation, there are some services where improvements are required. ROPA activity has increased with a shared register now in place. This review only included data processing sections of the ROPA with only minor issues identified. Our work did identify some control issues in relation to the prominence of privacy notices, signage for CCTV surveillance, and officer guidance for the privacy information that needs to be communicated during the operation of bodycams. These are set out in Appendix A. Due to the issues highlighted above, an **Adequate** assurance rating has been awarded for this review with actions for improvement detailed in the action plan at Appendix C. **Control Rating Key** **Full –** the Authority can place complete reliance on the controls. No control weaknesses exist. **Substantial** - the Authority can place sufficient reliance on the controls. Only minor control weaknesses exist. **Adequate** - the Authority can place only partial reliance on the controls. Some control issues need to be resolved. **Limited** - the Authority cannot place sufficient reliance on the controls. Substantive control weaknesses exist

Appendix A

Chorley Council					
Directorate	**Service Area**	**Service Specific Privacy Notice in place**	**DP requirements at point of collection**	**ROPA correctly populated**	**Comments**
Planning and Property	CCTV & Other Surveillance	N	N	Y	Privacy notice to be developed and publish information about CCTV on website. Provide alerts to the use of body worn camera. Update CCTV Code of Practice/operating procedures to incorporate body worn camera. Ensure signs are in situ in areas under CCTV surveillance and undertake periodic inspection process.
	Planning Applications / representations	N	Y	Y	Privacy Notice for planning applications and representations should be finalised & communicated.
	Adult Extra Care	P	Y	N	Tatton Gardens to be added to Privacy Notice. ROPA entry required.
Customer & Digital	Waste Collections / Green / Medical / Assisted	Y	Y	Y	
	Customer Complaints	N/A	N	N	Clearly communicate Privacy Notice in the complaint webpage/data capture form. ROPA entry is incomplete.
Change & Delivery	Consultations	Y	Y	N	ROPA entry does not show that personal data is processed.
Communities	Social Prescribing	N	N	Y	Privacy notice to be developed. Insufficient information currently provided. Develop script for social prescribers to ensure consistent provision of privacy information and consent notification.
	Activities - Health and Wellbeing: Courses Weight Management	Y	P	N	Include Privacy Notice in the course booking form (Event Brite). ROPA entry required.
	Homelessness	Y	Y	Y	
	Disabled Facilities Grant	Y	Y	Y	
	Minor Adaptions Grant	N/A	N	N	Privacy Notice should be issued following receipt of personal details from LCC. ROPA entry required.
Communications and Visitor Economy	Events	Y	N	N	Privacy Notice should be clearly communicated. ROPA entry required.
	Photography/ Filming/ Recording	Y	Y	N	Lack of Privacy Notice and corporate process for issuing and storing evidence of consent. This was rectified during our review; GDPR – Photography and filming report taken to/agreed by SLT (13th November 2023). ROPA entry required.

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

South Ribble Council					
Directorate	**Service Area**	**Service Specific Privacy Notice in place**	**DP requirements at point of collection**	**ROPA correctly populated**	**Comments**
Planning and Property	Facilities Management - CCTV	N	N	N	Privacy Notice to be developed and publish information about CCTV on website. Ensure signs are in situ in areas under CCTV surveillance. Update CCTV Policy to include role of Custodian. ROPA entry is incomplete.
	Facilities Management - Room Hire	N	N	N	Finalise and clearly communicate bookings Privacy Notice to data subjects. ROPA entry is incomplete.
	Planning Applications / representations	Y	Y	Y	
Customer & Digital	Neighbourhoods CCTV	N	N	Y	Privacy Notice to be developed and publish information about CCTV on website. Finalise and refresh CCTV Policy. Ensure signs are in situ in areas under CCTV surveillance and undertake periodic inspection.
	Waste Collections / Green / Medical / Assisted	Y	N	Y	Privacy Notice to be updated to include Permiserv processing and clearly communicated to data subjects.
	Customer Complaints	N/A	Y	N	ROPA entry is incomplete.
Change & Delivery	Consultations	Y	Y	N	ROPA entry does not show that personal data is processed.
Communities	Social Prescribing	Y	Y	Y	Privacy information is provided by the Social Prescriber during initial contact, however written guidance (the script) does not document this is given and will be updated.
	Activities - HAF and Adult Weight Management	P	N	Y	Finalise and clearly communicate service specific Privacy Notices to data subjects. Staff guidance to be developed.
	Homelessness	Y	Y	Y	
	DF Grant	Y	N	Y	Improve communication of Privacy Notice.
	Home Repairs Assistance Grant	Y	N	Y	Improve communication of Privacy Notice.
Communications and Visitor Economy	Key events (Music in the Park)	Y	N	N	Update MIP Privacy Notice to show SRBC is the data controller. Improve communication of the Privacy Notice to carer ticket applicants. ROPA entry required for events administration.
	Event Traders	N	Y	N	Generic events Privacy Notice to be developed, incorporating trader data. ROPA entry required.
	Photography/Filming/ Recording	Y	Y	N	Lack of Privacy Notice and corporate process for issuing and storing evidence of consent. This was rectified during our review; GDPR – Photography and filming report taken to/agreed by SLT (13th November 2023). ROPA entry required.

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

Appendix B

AUDIT ASSURANCE

Three Lines of Defence

Audit Area	1st Line	2nd Line	3rd Line	Internal Audit opinion
GDPR Transparency	Directorate Responsible Officers	Data Protection Officer	Internal Audit	Our review confirmed that reliance can be partially placed on the first line of defence, further work is required to proactively communicate privacy information.

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

Appendix C

MANAGEMENT ACTION PLAN

NO.	FINDING	AGREED ACTION	OFFICER & DATE
	Inform		
1	UK GDPR legislation places an obligation on the organisation to proactively make individuals aware of privacy information and give them an easy way to access it. Testing identified that 8 out of 15 SRBC, and 5 out of 13 CBC sampled service areas are not routinely directing data subjects to the privacy information at the point at which personal information is captured. To strengthen the Council's adherence to the first data protection principle 'lawfulness, fairness and transparency': • Access to the relevant privacy information should be provided up-front during the online application and other data capture processes. • The automated data protection telephone message should be reintroduced.	The Data Protection Officer (DPO) will liaise with the services identified to ensure the specific concerns highlighted in Appendix A are addressed, in particular that: • Access to the relevant privacy information should be provided up-front during the online application and other data capture processes. • The automated data protection telephone message should be reintroduced. Moreover, the DPO will take the report findings to the next SMT. Directors will be advised to check that privacy information is provided up-front during online application and other data capture processes for all their service areas, amending forms/processes if necessary, and provide confirmation back to the DPO.	Chris Moister June 2024

2	CCTV signs should alert data subjects that there is a surveillance system in operation and the reason for it. Our review identified partial compliance with this requirement: • CCTV signs are present in some but not all areas where cameras are present; • Some CCTV signs contain out of date information about the system operator and should be updated; • CBC only - privacy information should be provided when a body worn video system (bodycam) is in use. Currently, no warning (visual or verbal) is provided. These areas should be addressed as soon as practicable to ensure that people are aware that they may be recorded and to provide reassurance that the recordings will only be utilised for the purpose it is intended. Each Council's CCTV Code of Practice/Policy should be updated accordingly to reflect current arrangements.	The DPO will liaise with the services identified to ensure the specific CCTV concerns are addressed, in particular that: • CCTV signs are clearly displayed in all areas where cameras are present and periodically checked to ensure in situ. • CCTV signs are reviewed to ensure they are up to date and contain sufficient information. • CBC only - privacy information is provided when a body worn video system (bodycam) is in use (subject to outcome of Data Protection Impact Assessment). • Each Council's CCTV Code of Practice/Policy is updated accordingly to reflect current arrangements.	Chris Moister June 2024
3	Our work identified that service specific privacy notices should be considered for the following services that process and retain particular information: • CBC – CCTV (including body worn video), Planning, Social prescribing and events. • SRBC – CCTV, events and conference/other room hire.	The DPO will liaise with the services identified to ensure that service specific privacy notices are considered and developed for the following areas: • CBC – CCTV (including body worn video), Planning, Social prescribing and events. • SRBC – CCTV, events and conference/other room hire.	Chris Moister June 2024
	Processed		
4	A shared register of processing activity (ROPA) is in place to document the personal information is processed by each service and what the information will be utilised for. Sample testing	DPO will liaise with the services identified in Appendix A to ensure that the shared register of processing activity (ROPA) is completed to fully reflect all the data	Chris Moister June 2024

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'

	identified that the ROPA does not fully reflect all the data processed by each service with 7 out of 15 SRBC, and 7 out of 13 CBC entries missing or incomplete.	processed by each service. Each member of SMT will ensure that the shared ROPA is updated and accurately reflects current operational activity and provide quarterly confirmation to the DPO that the ROPA is actively maintained. The quarterly confirmation will be taken to the Information Security Council for consideration.	
5	Our review also identified that 5 SRBC, and 4 CBC services sampled do not currently have a process in place to ensure that personal data is deleted in accordance with the data retention policy.	The DPO will liaise with the services identified to ensure that they have a process in place to delete personal data in accordance with the data retention policy. Quarterly each member of SMT will ensure and provide confirmation to the DPO that data is deleted in accordance with the data retention policy. The quarterly confirmation will be taken to the Information Security Council for consideration.	Chris Moister June 2024

In accordance with the Public Sector Internal Audit Standards, internal audit has been the subject of an independent external assessment, which concluded that the 'internal audit activity conforms to the Standards'