GDPR

Peak District National Park Authority

Internal Audit Report 2018/19

Business Unit: Corporate
Responsible Officer: Director of Corporate Services
Service Manager: Head of Information Management & Data Development Manager (DPO)
Date Issued: 25 February 2019
Status: Final

	P1	P2	P3
Actions	**0**	**0**	**2**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Information is one of the most valuable assets held by any organisation. The authority should have adequate processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

The introduction of General Data Protection Regulations (GDPR) in May 2018 has increased the importance of effective controls surrounding information governance. GDPR has introduced additional mandated requirements to the Data Protection Act that it has superseded. Failure to meet these standards could result in a large fine up to the value of 4% of annual global turnover or €20 Million (whichever is greater).

An Information Governance audit carried out in 2017/18 identified that the authority had implemented an action plan to ensure that they had everything in place to ensure compliance with GDPR.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- The authority has sufficient policies and procedures in place to ensure GDPR compliance.
- The authority monitors the effectiveness of and compliance with these policies and procedures.

Key Findings

The Authority has taken the necessary actions to ensure that they are compliant with GDPR and have implemented monitoring arrangements to ensure that that they remain compliant.

The Authority is registered with the Information Commissioner's Office (ICO) as mandated. The Authority has appointed a qualified Data Protection Officer (DPO) who coordinates efforts to ensure that the Authority is complying with GDPR. The Authority have privacy notices for all key areas mandated by the ICO that sets out what data is being collected, why it is being collected, where the data is shared and the rights of individuals data is collected from. The privacy notices are easily accessible on the Authority's website and intranet.

The Authority have a range of policies that support GDPR compliance by setting out roles and responsibilities for keeping personal information secure, what actions must be taken and what systems are in place to ensure information security is maintained. All of the policies were updated in May 2018, with the exception of the CCTV policy. The Authority have provided data protection training to staff, e-mails / bulletins are sent to staff to raise awareness of data protection and the clear desk policy. The Authority has procedures in place in the event of a data breach and

these include steps to take for carrying out an impact assessment to decide whether to report to the ICO. Data breaches that have been reported internally are logged and assessments of the breaches are carried out to decide if further action is necessary.

Contracts with third parties have been updated so that they include a data protection clause and a data protection agreement with third parties that process the Authority's data. The Authority's employee contracts contain a data protection clause that mandates what data should be held securely.

The Authority has an information asset register that was compiled by the DPO and the information asset owners. In spring 2019 the Authority is migrating the data from a spreadsheet on to an application. The application will record a lot more detail about the information collected, including: where the information is kept, who the information is shared with and where the information is stored. The new application does not include fields for recording the security controls that are in place to protect data; this is something that should considered going forward. The new information asset register will help the Authority monitor the information that it holds and allow users to develop bespoke reports to assist information asset owners in fulfilling their responsibilities.

The Authority has developed a comprehensive retention schedule. There is currently no procedure in place to monitor that the retention policy is being adhered to. Once the information asset register application is in place, it would be possible to notify the information asset owners on what information is near to surpassing the retention period.

Freedom of Information, Subject Access and Environmental Information Regulation requests are logged and responded to in the correct time frame.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 CCTV Policy

Issue/Control Weakness	Risk
The Authority's CCTV policy has not been updated since the introduction of GDPR.	The policy is not compliant with GDPR.

Findings

The CCTV policy sets out how the CCTV data is recorded; how the information is logged and stored and the procedure for copying data and sharing data with third parties. However it has not been updated since 2015 to reflect and reference GDPR. The CCTV provider's certificate annexed to the CCTV policy has not been updated with the new certificate. The policy does not reference charges that could be applied for individuals that request to see CCTV.

Agreed Action 1.1

The CCTV policy is functional, but does require an update in order to become optimal. This update will take place during 2019 (by August 2019) including each of the items mentioned in the finding (reference to GDPR, updated certificate and reference to potential charges).

Priority	3
Responsible Officer	Environmental Management Officer/ Records and Information Manager
Timescale	31 August 2019

2 Data Retention

Issue/Control Weakness	Risk
The Authority does not have a procedure in place to monitor that the retention policy is adhered to.	The Authority are not complying with GDPR.

Findings

There is currently no monitoring procedure in place to ensure that the data held by the authority does not exceed the retention period.

The authority has an information asset register that was compiled by the authority's DPO and the information asset owners. The information asset register is currently on a Microsoft Excel spreadsheet. The data from the current asset register is being migrated to an application.

The new asset register flags up which data sets are nearing the end of the retention period and whether the information asset owner has disposed of the information. This should help to monitor that the data retention periods have been adhered to.

The authority should check that data has reached the end of its retention period has actually been destroyed and escalate data sets that have exceeded the retention period and still not been destroyed.

Agreed Action 2.1

The introduction of the Information Asset Register Software – InformU – will provide the mechanism for IAO's to monitor and manage data in relation to specified retention policies. This will include notifying the IAO's when data needs reviewing and requiring the IAO to log what action has been taken during the scheduled reviews.

Reporting from InformU will allow the Authority to monitor whether data is being kept up to date, whether the reviews are taking place and whether data is being disposed of once it is beyond its intended use and/or specified retention policies. The DPO and SIRO will coordinate the reporting, and will work with line managers if retention policies are found not to be adhered to in practice.

The 2019/20 financial year will provide a good baseline for this reporting, and the effectiveness of InformU in practice.

Priority	3
Responsible Officer	All IAO's
Timescale	30 April 2020

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.