Meeting:	Coast to Capital Audit and Risk Committee Meeting
Date:	Thursday 24 June 2021
Report Title:	Audit
Report by:	Jonathan Sharrock
Item No:	5
Part:	A

Recommendation:

The Committee is asked to:

- **Note** the status of the Audit Plan 2020/21 and Audit Plan 2021/22

1. Context

The Coast to Capital independent auditor left the organisation just before the internal reorganisation, and that role has not been continued under the new structure. The 21/22 business plan makes no explicit provision for future internal audits. Project audit in relation to LGF, GPF and GBF investments is the responsibility of the appropriate management teams. We will consider further as part of resource planning and with the Accountable Body whether there is any scope for continue audit work within the available resources.

2. Audit

There are two outstanding audits in relation to the **Audit Plan 2020/21** to report to the Committee:

- GDPR – a Management Response to this audit undertaken by BDO can be found in Annex A.
- Backing Business Fund – disappointingly Kreston Reeves has not delivered this audit by the expected timeframe (end March) and plan to submit their report in mid-June. Richard has stated that they were late in getting started but have commenced their work.

An annual audit report will be presented to the Board at the July Board meeting.

Background work has taken place on the approach to the **Audit Plan 2021/22** as discussed at the last meeting; however, given the continued uncertainty with

regards to the Business Plan over the last quarter an Audit Plan for this financial year cannot be prepared. Anna Meredith (Investments Audit and Compliance Officer) has left the organisation so there are also limited resources for internal audit to be delivered at this current time. The Accountable Body is required to agree the Audit Plan for 2021/22; therefore, further discussions on the approach need to take place.

There is no budget allocated to audit in 2021/22.

3. Next Steps

This programme of work will be led by the new Programme Manager and the Accountable Body client management will be led by the new Corporate Manager.

4. Diversity Statement

There are no diversity considerations to raise.

5. Legal Statement

This paper has been reviewed by Brighton and Hove City Council in their role as the Accountable Body.

6. Financial Statement

There are no financial implications to consider.

Annexes:

- **Annex A** – GDPR Audit and Management Response

Further information on request:

- None

COAST TO CAPITAL

GDPR AUDIT REPORT – DRAFT

GDPR AUDIT
MARCH 2021

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Moderate	**Moderate**

DISTRIBUTION	
Katie Nurcombe	Head of Corporate Affairs
Kristel Smith	Data Protection Manager

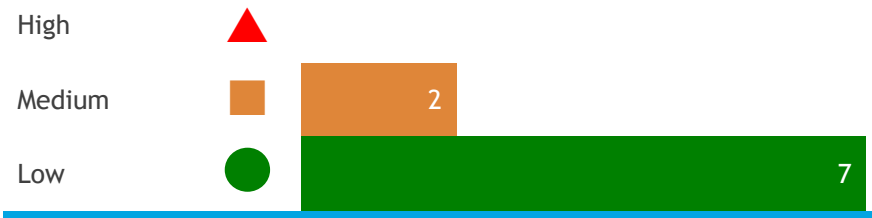
REPORT STATUS LIST	
Auditor:	Louise Sadler
Dates work performed:	1 - 5 February 2021
Draft report issued:	25 March 2021
Final report issued:	TBC

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

Design	Generally a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Evidence of non-compliance with some controls that may put some of the system objectives at risk.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)



TOTAL NUMBER OF RECOMMENDATIONS: 9

BACKGROUND:

Coast to Capital is one of numerous Local Enterprise Partnerships (LEPs) across England. It is a business led partnership between local authorities and businesses, and plays a central role in determining local economic priorities and undertaking activities to drive economic growth and the creation of local jobs. BDO was asked to complete a review of data protection (GDPR) compliance arrangements.

Overall, Coast to Capital has low exposure to personal data. Coast to Capital employs 35 staff, and so the majority of personal data processing relates to maintaining the workforce. There is some personal data held within the CRM system, in relation to the local businesses which Coast to Capital supports, however the CRM system primarily holds business data.

Coast to Capital are not required by law to appoint a Data Protection Officer (DPO), but have appointed the PA to Chief Executive and Office Manager with the responsibility for GDPR compliance, as Data Protection Manager. The Data Protection Manager leads GDPR compliance and is supported by data champions within each business area. Data Champions act as the local point of contact for personal data related queries, and ensure that key data protection compliance messages are cascaded throughout the organisation at monthly team meetings. Coast to Capital has engaged Uptime Solutions as their outsourced IT provider, who provide a hosted desktop system, email services and authentication.

At the time of reporting, Coast to Capital had received one subject access request in November 2019. This was confirmed as being processed and responded to within the 30 day time limit. To date, Coast to Capital have not recorded any data breaches.

SCOPE AND APPROACH:

We interviewed key individuals who are involved with GDPR compliance including the Data Protection Manager, Data Champions, the Communications Manager, Head of Services and a representative from Uptime Solutions, Coast to Capital's outsourced IT provider.

Relevant policies, procedures and other compliance documentation were reviewed, to assess the overall level of data protection risk across Coast to Capital, to determine whether risks were appropriately addressed, documents were aligned to the GDPR requirements, and to understand the current control environment. We interviewed key individuals involved with

data privacy and performed a remote walkthrough of the CRM system to understand the process for capturing consents and marketing preferences.

GOOD PRACTICE:

During the course of our review, we identified the following areas of good practice:

- There appears to be an effective data protection training and awareness program in place. At the time of the review, we confirmed that 100% of staff have completed the mandatory GDPR e-learning module.
- GDPR compliance is led by the Data Protection Manager (also the PA to the Chief Executive and Office Manager), who is supported by Data Champions in each department.
- The Data Protection Manager and Data Champions meet bi-monthly to discuss compliance queries within the departments, and key compliance areas, i.e. forthcoming projects where a DPIA is required, and ensuring that data sharing agreements are on file.
- The Data Protection Manager has been awarded the EU General Data Protection Regulation Foundation with the International Board for IT Governance.
- Key GDPR policies and procedures are easily accessible to staff and published via the centralised SharePoint.

KEY FINDINGS:

Notwithstanding the areas of good practice identified above, we have raised two findings of medium significance and seven findings of low significance. The medium findings relate to the following:

- Coast to Capital has not formally documented an up-to-date information asset register (IAR), which forms the foundation of GDPR governance and compliance. As a result, the Data Protection Manager does not have full oversight of data processing activity across the organisation, including the processing purpose, data processed, lawful basis for processing, processing of special category data, data processors/joint controllers (with whom personal data is shared), and their location. Documenting data processing activity is a key requirement of the GDPR. The development and maintenance of the IAR is a significant part of any GDPR program and drives the overall implementation and ongoing compliance requirements of the regulation.

- Emails are currently retained indefinitely, increasing Coast to Capital's exposure in the event of a data breach. The GDPR requires organisations to hold personal data only for as long as it is needed. If Coast to Capital retains emails indefinitely, then the organisation is unlikely to adhere to the storage limitation principle of the GDPR. Furthermore, implementation of a documented retention period for emails makes it easier to locate specific data in response to a subject access request.

CONCLUSION:

In view of the organisation's limited exposure to personal data, overall Coast to Capital has implemented a reasonable infrastructure required for GDPR compliance. However, some improvements are required. The majority of findings within this report highlight gaps or weaknesses in relation to organisational oversight of data processing activities and reflecting data processing activity appropriately in supporting policies. The remaining findings relate to documenting compliance requirements internally i.e. the process for granting data subject rights requests, reporting and managing data breaches and demonstrating continued compliance with the regulation.

Despite the findings raised, with the existing mitigations in place and overall limited exposure to personal data, we have determined that there is generally a sound system of

internal control, designed to achieve system objectives. Therefore, we are able to provide moderate assurance in relation to the design of the controls in place to manage and mitigate any data protection compliance risk.

We did however identify some areas of non-compliance with key procedures and controls which has led to recommendations to strengthen existing arrangements, as reflected in the findings. A key objective of a sound data protection control framework is to ensure compliance with the data protection regulation and the principles that govern it, ensuring that the personal data processed by Coast to Capital is secure, and the rights and freedoms of data subjects are not compromised, however taking into account the overall exposure to personal data across Coast to Capital and a good number of areas of good practice that were verified during the review, we are able to provide moderate assurance in relation to the operational effectiveness of the controls in place to manage and mitigate any data protection compliance risk.

DETAILED FINDINGS

RISK: LACK OF VISIBILITY OF COAST TO CAPITAL'S DATA PROCESSING ACTIVITIES ALONG WITH THE INFORMATION DATA FLOW AND THE LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION

Ref	Sig.	Finding
1		**Coast to Capital has not formally documented an Information Asset Register (IAR)** The review highlighted that Coast to Capital has not formally documented their data processing activity through an IAR (also known as a Record of Processing Activity). The IAR forms the foundation of GDPR governance and compliance. Discussions indicated that during GDPR implementation, Coast to Capital were provided with templates to develop the IAR, however these were overly complex and not conducive to providing the Data Protection Manager with appropriate oversight of data processing activity, across the organisation. Although Coast to Capital has a low exposure to personal data processing, discussions confirmed that the existing templates have not been updated since inception, which on the arrival of a recently appointed Data Protection Manager resulted in a new attempt to update and build an IAR for Coast to Capital that was representative of current data processing activity across the organisation. The GDPR and the ICO states that organisations are required to document data processing activities. In the absence of a centralised, formally documented IAR which documents the processing purpose, types of personal data processed, the lawful basis for processing, and identifies (among other things) special category data, third party data processors and their location (UK, EEA or outside EEA), there is an increased risk that GDPR compliance efforts will not fully reflect overall data processing across the organisation, and the Data Protection Manager will not have full oversight of instances where data is shared with external organisations. It is important to note that the IAR typically drives the whole GDPR implementation and ongoing compliance program. Organisations that have formally documented and have good visibility on data processing activity across the organisation can prepare and issue policy and procedures comfortable in the knowledge that they align to the information collected within the IAR.

RECOMMENDATION:

Recommended that Coast to Capital enhance the data mapping document developed for Communications and corporate affairs to include the following columns:

- Data processing purpose
- Category of data subject (i.e. current/former employee, recruitment applicant)
- Personal data processed (i.e. name, email, home address)
- Lawful basis for processing
- Special category data
- Children's data
- Criminal conviction data
- Location of the data (internal systems)
- Named recipients of personal data (third party data processors or joint controller scenarios)
- Location of third party data processors (UK, EEA or outside EEA)
- Retention period

It is important to note that the old template that was previously completed is still considered to be a useful tool in building an up to date IAR. This document included a lot of useful and relevant information that can be placed into the new IAR, however caution needs to be given to how up to date this information is. It is suggested that the Data Protection Manager meets with key stakeholders across the key functions to determine which information is still relevant and can continue to be used and what information is considered to be out of date.

Once developed the Data Protection Manager will have a comprehensive oversight of data processing activity across Coast to Capital. Use of drop down menus (i.e. for lawful basis for processing) should be used to ensure consistency, and version control to demonstrate that the IAR is regularly reviewed and updated should also be included.

When the IAR has been reviewed an updated, Coast to Capital should complete a reconciliation to ensure that data sharing agreements are on file for all identified third party data processors and any joint controller relationships that exist.

MANAGEMENT RESPONSE:

This will be our main focus following this review and the Data Protection Manager will work on the creation of a suitable IAR. This will then be passed to the Data Champions to complete for their individual teams and checked by the Data Protection Manager.

Responsible Officer:	Kristel Smith
Implementation Date:	August 2021

RISK: NON-COMPLIANCE WITH GDPR AND THE MAIN PRINCIPLES THAT ARE INCLUDED WITHIN THE REGULATION, WHICH ULTIMATELY COULD LEAD TO FINANCIAL SANCTION OR REPUTATIONAL RISK FOR COAST TO CAPITAL		
Ref	Sig.	Finding
2		**Emails are currently retained indefinitely, increasing Coast to Capital's exposure in the event of a data breach** Coast to Capital maintains a data retention policy, which documents the type of record/document, reason held, minimum retention usually required, recommended retention period, reason for recommended retention period and where information held, however discussions indicated that currently emails are held indefinitely. The GDPR requires organisations to hold personal data only for as long as is reasonably required. If Coast to Capital has not formalised a retention period for email retention, and emails are held indefinitely, then Coast to Capital are unlikely to meet the requirements of the storage limitation principle built into the GDPR. Furthermore, indefinite retention of emails also presents additional risks. These include Coast to Capital not having complete oversight of emails held within the systems but also in a data breach scenario, there is currently a lot more information available to be compromised as opposed to implementing an email retention policy which would reduce this risk significantly. It is also worth noting that if Coast to Capital were to receive a subject access request, the requirement would be to search all emails. Implementing and adhering to a formalised email retention period would therefore reduce the potential scope (and therefore time taken) to respond to a subject access request.

RECOMMENDATION:
Recommended that Coast to Capital agree and document the retention period for emails within the retention schedule and ensure that the adherence to this policy is regularly tested. Coast to Capital should also consider whether emails should be manually or automatically deleted after a prescribed period.

MANAGEMENT RESPONSE:	
Following the move from our hosted system to Microsoft 365, we are already in discussions to implement an email retention policy that will auto delete all emails more than 12 months old (subject to retaining emails required for legal reasons).	
Responsible Officer:	Kristel Smith
Implementation Date:	July 2021

RISK: A LACK OF TRANSPARENCY IN COMMUNICATION WITH INTERNAL AND EXTERNAL DATA SUBJECTS ON THE DATA PROCESSING ACTIVITIES OF COAST TO CAPITAL		
Ref	Sig.	Finding
3		**Privacy notices do not accurately communicate data processing to data subjects** Coast to Capital has developed a general privacy notice, published via the website, and a privacy notice for staff, however discussions indicated that Coast to Capital also processes personal data regarding recruitment applicants (albeit for a limited period of time) and board members. Currently, the published privacy notices do not communicate how the personal data for both groups is processed. This is not in-keeping with the transparency principle, whereby data subjects should be able to access the necessary information informing them of how and for what reason Coast to Capital processes their personal data. Individuals have the right to be informed about the collection and use of their personal data. In the absence of clear, complete and accessible privacy notices, which communicate data processing activity to all categories of data subjects, Coast to Capital is not being clear, open and honest with data subjects about how their data is used.

RECOMMENDATION:
Subsequent to the development of the IAR (refer to finding 1) and confirmation of the different categories of data subjects that Coast to Capital process information on behalf of, it is recommended that Coast to Capital review and update existing privacy notices (external and internal), to ensure that they accurately communicate all data processing activity as documented within the IAR. Going forward, it is important that periodic reviews of the IAR are completed and any changes are reflected in the privacy notices ensuring that the requirements of the transparency principle is met. In addition this it is recommended that an additional privacy notice is developed to cover any information processed on behalf of recruitment applicants and that this is provided to relevant applicants at the time of them providing their personal information.

MANAGEMENT RESPONSE:	
The Data Protection Manager will create a privacy notice for recruitment applicants to be displayed on the website and will work with the Governance Officer to create a Board member privacy notice which will be included as part of their induction.	
Responsible Officer:	Kristel Smith & Nick Darwin
Implementation Date:	September 2021

RISK: POTENTIAL BREACH OF INDIVIDUAL'S RIGHTS IF COAST TO CAPITAL DOES NOT HAVE A ROBUST POLICY AND PROCEDURE FRAMWORK IN PLACE TO ADDRESS ANY REQUESTS/INCIDENTS		
Ref	Sig.	Finding
4		**The Coast to Capital CRM system does not distinguish between data subjects marketing preferences** Discussions indicated that currently the CRM system captures data subject's consent (including time and date stamp) and marketing preferences. Despite this, it was confirmed that there is also a subsection of contacts within the CRM system who have engaged with Coast to Capital in the past for other reasons, and have also been added to the CRM system to receive communications, however those individuals have not necessarily provided consent to receiving marketing information. The CRM does not currently distinguish between individuals who have engaged with Coast to Capital, but stated no marketing preferences and those individuals who have unsubscribed (or removed consent) to receiving marketing information. If the CRM does not clearly and easily distinguish between data subject preferences, there is an increased risk that either Coast to Capital is not able to fully reach contacts, or a risk that individuals who have removed consent/unsubscribed may be accidentally sent marketing information which may result in a regulatory consent management breach.

RECOMMENDATION:
Whilst we appreciate that the risk is low, it is recommended that Coast to Capital review the marketing preferences and consent capabilities with the current CRM system, in order to distinguish between: • Individuals who have solely provided consent to process personal data • Individuals who have provided to consent to process personal data and would like to receive marketing information • Individuals who have unsubscribed from receiving marketing information going forward

MANAGEMENT RESPONSE:	
The Communications Manager will work with Evolutive to ensure consent capabilities work fully and to ensure marketing communications are only sent to those who have provided consent.	
Responsible Officer:	Jake Daniels
Implementation Date:	September 2021

RISK: POTENTIAL BREACH OF INDIVIDUAL'S RIGHTS IF COAST TO CAPITAL DOES NOT HAVE A ROBUST POLICY AND PROCEDURE FRAMEWORK IN PLACE TO ADDRESS ANY REQUESTS/INCIDENTS		
Ref	Sig.	Finding
5		**Coast to Capital has not documented internal procedures for granting data subject rights requests** The GDPR grants data subjects a number of rights which include the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to portability, right to object and rights in relation to automated decision making and profiling. At the time of the review, Coast to Capital have only ever received one subject access request, which we confirmed was completed within the required 30 day time limit. Discussions indicated Coast to Capital has not formally documented internal procedures which govern how a data subject right would be processed internally. We recognise Coast to Capital has overall low exposure to personal data and that only one data subject rights request has been received, however, in the absence of a formally documented procedure, there is an increased risk that in the event of complex requests, staff turnover or absence, future data subject rights requests will not be processed within the required 30 day time scales.

RECOMMENDATION:

Recommended that Coast to Capital develop internal procedures (or process maps) which document the step by step internal process to follow, in the event that the organisation receives a data subject rights request. Internal procedures should include verifying an individual's identity, instances in which a subject access request can be refused, locating and extracting the data from relevant systems (as detailed in the IAR), redacting documents and sending to/notifying the data subject, as appropriate.

We also identified the following additional columns we recommend should be added to the Subject Access Request Log, to provide the Data Protection Manager with greater oversight of the management of data subject rights requests going forward:

- Nature of the data subject rights request (i.e. access, rectification, deletion)
- Deadline for completion
- Number of days taken to complete the request
- Whether the request was completed within the prescribed 30 day time limit

MANAGEMENT RESPONSE:

Documents to be produced by Data Protection Manager, using templates provided by BDO, working alongside Uptime to ensure instructions on locating data is correct.

Responsible Officer:	Kristel Smith
Implementation Date:	September 2021

RISK: ABSENCE OR INEFFECTIVENESS OF ORGANISATIONAL AND TECHNICAL CONTROLS TO SATISFY SECURITY OF PERSONAL INFORMATION PROCESSED OR INDEED TO REACT IN THE EVENT OF A DATA BREACH INCIDENT		
Ref	Sig.	Finding
6		**Coast to Capital has not documented processes for reporting and managing data breaches** The GDPR imposes a mandatory requirement on all organisations to report all risk assessed data breaches to the supervisory authority within 72 hours of becoming aware of the breach. In addition to this, organisations are also required to maintain a record of all data breaches, regardless of whether there is the requirement to notify the supervisory authority or not. At the date of the review, no data breach incidents had been reported by Coast to Capital to the supervisory authority. Although, Coast to Capital do have a data breach policy in existence, our review confirmed that there was limited guidance included on the procedure to follow in such a scenario. In the absence of formally documented procedures which govern the process to follow for reporting a data breach, assessing the severity of the breach and reporting to the ICO and/or the data subject there is an increased risk that Coast to Capital will not meet the 72-hour timeframe for reporting, in the event of a serious data breach. Coast to Capital should therefore have a robust breach detection, investigation and internal reporting procedure in place, which is widely communicated to staff. Further discussion also confirmed that Coast to Capital have not developed a data breach log for recording data breach incidents. In addition to demonstrating compliance with the requirement to document all data breach incidents internally, a log can also serve as a useful tool for the Data Protection Manager, to ensure compliance with key reporting timeframes and highlight key insights specific to the incidents that have been recorded i.e. the common root cause of a data breach incident and any useful notes that provide an explanation on progress and the eventual outcome.

RECOMMENDATION:

Recommended that Coast to Capital develop an internal procedure which provides clear guidance on the process to follow, in the event of a data breach incident. Internal procedures should include the roles and responsibilities of staff, assessing the severity of a data breach (based on number of individuals affected and the nature of the data breached) and the process for reporting a data breach to the ICO and/or data subject.

Coast to Capital should also develop a data breach log which captures the following:

- Data breach reference number
- Date and time data breach identified
- Name and department of the individual who reported the data breach
- Description of the data breach
- Estimated number of individuals affected
- Whether the data breach included special category data
- Description of the likely consequences of the data breach
- Measures taken as a result of the identified data breach
- Whether the data breach was reported to the ICO (including date and time)
- Whether the data breach was reported to the individuals affected
- If the data breach was reported to the ICO, whether this was completed within 72 hours of Coast to Capital becoming aware of the data breach

MANAGEMENT RESPONSE:

Documents to be produced by Data Protection Manager using templates provided by BDO.

Responsible Officer:	Kristel Smith
Implementation Date:	September 2021

RISK: ABSENCE OR INEFECTIVENESS OF ORGANISATIONAL AND TECHNICAL CONTROLS TO SATISFY SECURITY OF PERSONAL INFORMATION PROCESSED OR INDEED TO REACT IN THE EVENT OF A DATA BREACH INCIDENT		
Ref	Sig.	Finding
7		**Coast to Capital has not formally documented an information security policy** One of the key principles of GDPR is to ensure that organisations have appropriate technical and organisational measures are in place to protect personal data. Currently, the data protection policy details a number of physical security measures to keep personal data safe, which includes storage, prohibition of the use of removable media, use of passwords and staff responsibilities relating to the security of physical assets i.e. that filing cabinets containing personal data remain locked. Coast to Capital has outsourced IT services to an organisation called Uptime Solutions, who provide a hosted desktop system which includes email services and authentication. As part of outsourcing arrangements, Uptime Solutions will have implemented a number of technical security measures in place to protect personal and commercially sensitive data, however the review highlighted that information security measures have not been formally documented by Coast to Capital. In the absence of formally documented information security measures, there is an increased risk that the Data Protection Manager will not have full oversight of information security arrangements to be able to determine whether arrangements are sufficient and fit for purpose in respect of the current data processing activity present across the organisation.

RECOMMENDATION:
Recommended that Coast to Capital formally documents an information security policy which includes a list of the technical and organisational measures in existence to protect personal data. Furthermore, and to achieve this objective, we would suggest that Uptime Solutions are asked to contribute to the information security policy. Once formalised, the Data Protection Manager can periodically review measures in place, to determine whether current arrangements are appropriate, but more importantly there will be a physical information security policy that can be disseminated to Coast to Capital staff that clearly sets out the organisational policy in respect of information security which can be applied to their day to day responsibilities.

MANAGEMENT RESPONSE:	
Following the move from our hosted system to Microsoft 365, we are already in discussions with uptime to create this policy and update all IT related policies.	
Responsible Officer:	Kristel Smith
Implementation Date:	July 2021

RISK: LACK OF VISIBILITY OF COAST TO CAPITAL'S DATA PROCESSING ACTIVITIES ALONG WITH THE INFORMATION DATA FLOW AND THE LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION		
Ref	Sig.	Finding
8		**Data Protection Manager does not have full oversight of instances where Coast to Capital relies on legitimate interest as the lawful basis for processing** As documented in finding 1, Coast to Capital has not developed an IAR, of which one of the requirements is that organisations are to maintain a record of the lawful basis for processing, for each data processing activity. The review confirmed that there have been instances in which Coast to Capital has relied on legitimate interest as the lawful basis for processing personal data and furthermore that legitimate interest assessments have not been completed in all instances. Currently, because Coast to Capital has not documented the lawful basis for processing for all data processing activity across the organisation within an up-to-date IAR, the Data Protection Manager does not have complete oversight of instances in which legitimate interest assessments should be documented. Whilst the risk is considered to be low, in the absence of formally documented legitimate interest assessments for all data processing activity in which legitimate interest is cited as the lawful basis for processing, Coast to Capital cannot evidence that it has considered the interests of the organisation against the rights of the data subject.

RECOMMENDATION:
For completeness, and to ensure that Coast to Capital can evidence that it has considered the interests of the organisation versus the rights of the data subject, upon completion of the updated IAR, Coast to Capital should review all instances where legitimate interest is cited as the lawful basis for processing personal data and ensure that legitimate interest assessments have been completed.

MANAGEMENT RESPONSE:	
This recommendation will be actioned following the completion of the IAR.	
Responsible Officer:	Kristel Smith
Implementation Date:	September 2021

RISK: LACK OF OWNERSHIP/ACCOUNTABILITY ACROSS COAST TO CAPITAL IN RESPECT OF DATA PROTECTION RSPONSIBILITY AND A LIMITED UNDERSTANDING OF COAST TO CAPITAL'S RISK PROFILE IN RESPECT OF THE PERSONAL INFORMATION PROCESSED		
Ref	Sig.	Finding
9		**Coast to Capital cannot evidence ongoing compliance with the requirements of GDPR** As part of the fieldwork we confirmed that the Data Protection Manager holds periodic meetings with the data champions to discuss pertinent issues within the individual departments. Whilst we acknowledge that Coast to Capital has low exposure to personal data, we noted that a GDPR compliance plan which ties together key areas of GDPR compliance and demonstrates on-going accountability and compliance with the regulation, has not been developed. In the absence of an on-going data privacy compliance plan, there is a risk that key areas of GDPR compliance will not be regularly reviewed and updated.

RECOMMENDATION:

Recommended that Coast to Capital should develop an annual plan which includes, but is not limited to:

- Annual review of key policies and procedures
- Review of the information asset register
- Review and update privacy notices to predominantly reflect changes in the IAR
- Annually refresh GDPR awareness training
- Annual data cleanse per the data retention schedule
- A testing schedule to ensure that the policies and procedures are being adhered to across the organisation

MANAGEMENT RESPONSE:

Following the previous recommendations being implemented, an annual plan will be created and then shared with Data Champions and wider team. As part of this plan, quarterly reminders to staff regarding GDPR and our responsibilities. Refresher training to be completed by all staff.

Responsible Officer:	Kristel Smith
Implementation Date:	October 2021

OBSERVATIONS

VERSION CONTROL

We noted inconsistencies in the use of version control across data protection policies and procedures. To demonstrate regular review and ensure standardisation, Coast to Capital should ensure documents are issued with a publication date and due for review date.

TRAINING AND AWARENESS

Whilst we noted that 100% of staff have completed the GDPR training module, Coast to Capital could consider enhancing employee knowledge in specific areas of higher risk, such as periodic reminders of the internal process for reporting data breaches and subject access requests.

In addition, whilst we recognise that Coast to Capital has 100% completion for the e-learning GDPR module, discussions indicated that the training will in future be rolled out annually. For completeness, Coast to Capital should include the requirement for staff to refresh GDPR training annually in the data protection policy.

DOCUMENTING DATA PROTECTION MANAGER ARRANGEMENTS

Coast to Capital have concluded that the organisation is not required to appoint a compulsory Data Protection Officer (DPO), because it has limited exposure to personal data processing activity. However, for completeness, Coast to Capital should consider formally documenting why the organisation doesn't meet the criteria for appointing a DPO, and to formalise internal arrangements to demonstrate compliance with the accountability principle.

STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.

Kristel Smith	Office Manager & PA to the Chief Executive
Jake Daniels	Communication Manager
Malcolm Brabon	Head of Services
Marsha Robert	Data Champion
Luke West	Data Champion
David Smith	Data Champion
Roy Martin-Harris	Uptime Solutions

APPENDIX I - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non-compliance with some controls that may put some of the system objectives at risk.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non-compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE	
High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX II - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The objective of the audit is to provide assurance to the Audit Committee on whether Coast to Capital has addressed their responsibilities in respect of GDPR, have an adequately designed and operating data-protection control environment in place, and to identify any improvements in compliance, which Coast to Capital will need to address going forward.

KEY RISKS:

The key risks with this area of activity are:

- Non-compliance with GDPR and the main principles that are included within the regulation, which ultimately could lead to financial sanction or reputational risk for Coast to Capital.
- Lack of employee buy in to be able to deliver and embed Coast to Capital's data protection policies and procedures.
- Lack of visibility of Coast to Capital's data processing activities along with the information data flow and the legal basis for processing personal information.
- A lack of transparency in communication with internal and external data subjects on the data processing activities of Coast to Capital.
- Potential breach of individual's rights if Coast to Capital does not have a robust policy and procedure framework in place to address any requests/incidents.
- Absence or ineffectiveness of organisational and technical controls to satisfy security of personal information processed or indeed to react in the event of a data breach incident.
- Lack of ownership/accountability across Coast to Capital in respect of data protection responsibility and a limited understanding of Coast to Capital's risk profile in respect of the personal information processed.
- Failure to safeguard against any exposures to data sharing to include third party contract risk and third country data transfer risk.

SCOPE:

The following areas will be covered as part of our review:

Area	Description	GDPR Articles Covered
Awareness	Employee awareness of GDPR and the corresponding regulations along with Council and key committee awareness of new accountability requirements	Article 5
Information you hold	Understanding personal information held and the reasons for this	Articles 5, 9, 10, 30
Joint controllers	Understanding any joint controller relationships in existence and reviewing contractual obligations	Article 26
Processors	A review of third party processor relationships in existence and consideration of contractual requirements and due diligence expectations	Articles 28, 29
Communicating privacy	Communicating information regarding data processing	Articles 5, 12, 13, 14
Individual rights	Maintaining an individual's rights under GDPR, including data portability	Articles 15, 16, 17, 18, 19, 20, 21, 22
Legal basis for processing	Aligning processing with a clear legal basis and justification	Article 6
Consent	Wording, clarity and existence of consents along with the consent management processes in existence in respect of the collection and removal of consent	Article 7
Children	Parental and guardian consent in place, where required	Article 8
Data breaches	Processes to identify, report and manage a data breach	Articles 33, 34
Privacy risk	How THF has considered the data protection landscape and the associated risks along with mitigation methodologies	Articles 5, 25, 35, 36
Data protection officer (DPO)	Justification regarding the requirement for a DPO or not, along with a review on independence, the DPO role and their corresponding responsibilities	Articles 37, 38, 39
International data transfers	Exposure to international transfers of personal data and the corresponding safeguards	Articles 45, 46, 47, 48, 49

Accountability	Review in relation to how THF is continuing to demonstrate accountability in the area of privacy and data protection	Articles 5, 24
Information security	Summarising the information security environment and the associated measures in place across the organisation	Article 32
Processing for archiving purposes	An understanding of any processing activities that involve archiving and that the data protection regulation has been adequately applied to these	Article 89

APPROACH:

The review will be conducted remotely. Interviews and discussions will be undertaken by MS Teams or similar. Documents will be provided electronically for review. There will be no visits to Coast to Capital premises. It is assumed that there will be approximately five people to interview.

The approach to assessing the design of the controls in place will be as follows:

- We will interview a sample of individuals that have had a role in developing Coast to Capital's GDPR approach. We will use our privacy compliance framework tool, which covers all of the GDPR regulatory requirements to assess Coast to Capital's awareness and implementation of the regulatory requirements (focusing on the Articles above).
- We will review relevant policies and procedures and assess whether these are aligned with GDPR requirements.

FOR MORE INFORMATION:

CHRISTOPHER BEVERIDGE

ROBERT NOYE ALLEN

Christopher.beveridge@bdo.co.uk

Robert.noye-allen@bdo.co.uk

www.bdo.co.uk