GoodCorporation Standard Assessment Report (Data Protection)

VERCO plc

August 2016

CONFIDENTIAL – for authorised distribution only

The measure of a good company

Organisation:	Verco
Activity:	Telecommunications and Internet Services
Principal contact:	Jane Smith
Sites visited:	Headquarters and 4 branches in London, Birmingham, Bristol and Newcastle.
Date of assessment:	1 - 19 August 2016
Assessors:	Gareth Thomas and Till Lembke
Document reference:	Verco-DP Report-Template.doc
Document status:	Final

Contents

Introduction

Verco is VERCOMMUNICATION Company's largest dealer in the UK and it is 100% owned by the group. Verco employs over 800 people in the UK, across 40 stores. Verco sells new handsets and other telecommunication devices, internet and mobile data connections as well as television and entertainment connection packages. Products and services are sold to business customers and directly to the retail market.

Verco also runs an aftercare business, providing servicing to new and used devices and a network of engineers who visit customer on site to help install any new lines or infrastructure needed to obtain online access.

In 2015 the business made a commitment to be evaluated according to the GoodCorporation Data Protection Framework under the leadership of its head of marketing and e-commerce Jane Smith. The business undertook an initial review of its operations against the Standard in 2015 and then undertook a full assessment in August 2016, the results of which are summarised in this report.

The GoodCorporation Data Protection Framework consists of a list of good data protection practices and can be used to design, embed and evaluate an organisations' data protection system and culture.

The GoodCorporation Data Protection Framework

The GoodCorporation Data Protection Framework is set out in Appendix I of this report. It provides the criteria for this assessment report. Based on a core set of principles for responsible data management, the framework sets out 76 areas of management practice that are assessed to determine how well the organisation performs against each. The GoodCorporation Data Protection Framework covers ten key areas of management:

- Management and governance;
- Risk assessment;
- Security environment;
- Legal environment;
- Operational data practices;
- Managing employees who handle data;
- Managing routine access by third parties;
- Managing requests;
- Breaches; and
- Monitoring and review.

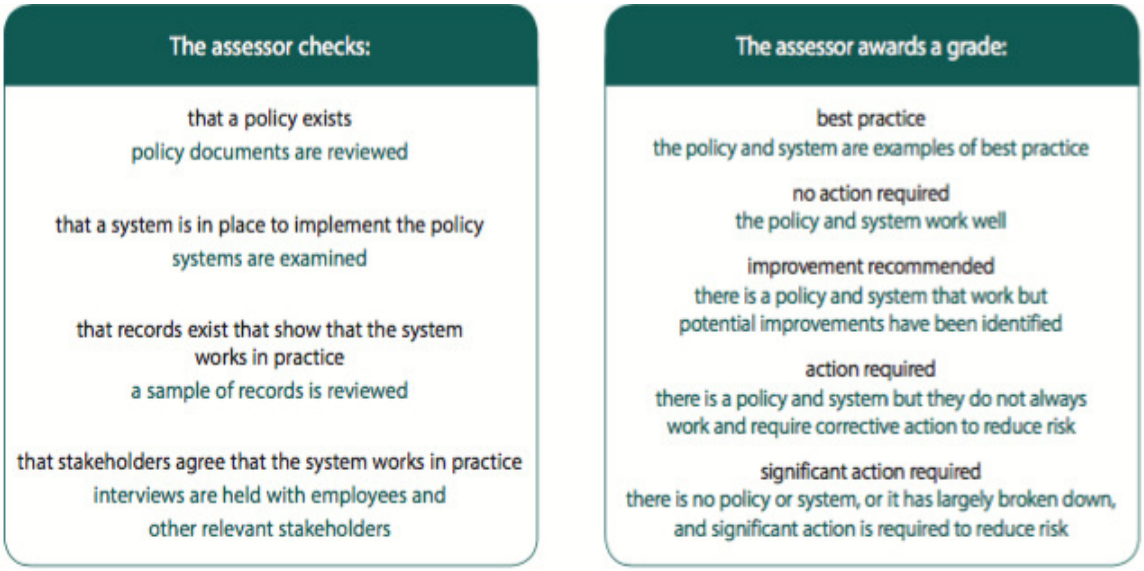
This assessment was conducted against the GoodCorporation Data Protection Framework (August 2016 Revision).

Assessment process and grading

The assessment took place in Verco's London headquarters and four branches each in London, Birmingham, Bristol and Newcastle, between 1st-19th August 2016, and included a number of telephone interviews. The assessor reviewed documents, interviewed functional managers, and interviewed samples of stakeholders including employees, service providers and business partners to evaluate Verco's overall adherence to the GoodCorporation Standard for data protection.

All stakeholder interviews were conducted in confidence and this report does not attribute individual comments. Where problems were found or sensitive feedback was given this has necessarily been stated in general terms unless specific consent was granted to give details of individual cases.

Each evidence point was assessed, and graded according to a scale as shown here:



Please note: 'best practice' corresponds to 'commendation', 'no action required' corresponds to 'merit', 'improvement recommended' corresponds to 'observation', 'action required' corresponds to 'minor non-compliance' and 'significant action required' corresponds to 'non-compliance'.

Overall outcome

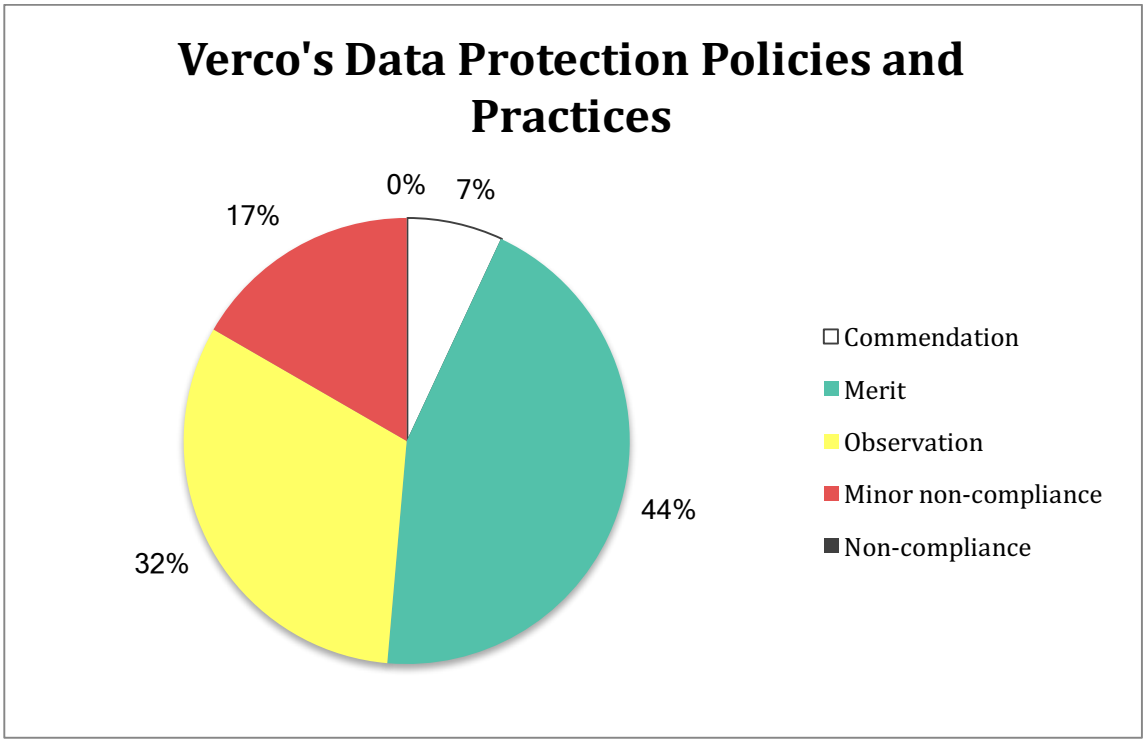
Executive Summary

Verco has obtained merits or commendations in just over half of the assessed practices. In five practices, Verco has demonstrated exemplary conduct. Its policies on data protection are particularly commendable (MG1), as is its approach to risk assessments to consider data protection risks (RA1), which are thoroughly conducted on a regular basis. In addition, Verco is very strong in compiling guidelines which are clear and comprehensive, and include sections on, *inter alia*, identifying vulnerable customers, practical tips on how to engage with them, specific considerations for frontline staff, and guidance on how their personal data should be protected (OP8). The processes employed to destroy data or to render it irrecoverable are also of a very high standard (OP21). Finally, Verco has succeeded in conveying clearly whom to speak to in case of a suspected data breach, and all employees interviewed bar one have a clear and accurate idea of whom to address should they suspect any data breach (BR2).

Conversely, just under a fifth of Verco's practices which benefit from a policy or a system do not always work, and require corrective actions to reduce risk. This includes a lack of clarity in relation to privacy notices (MG4), negligent locking of cabinets (PS2), and a relaxed approach to the use of non-encrypted USB devices (IS5) and training on information systems security (IS8). Four operational practices, touching on consent (OP1), data collection (OP4), privacy notices for children and other vulnerable individuals (OP10) and the monitoring of employees; use of internet, email and other communication systems (OP13), would especially benefit from improvements. In addition, job-specific training for relevant employees would be recommended (ME1). Verco's engagement with services providers' or business partners' data protection practices and verification thereof (TP2 and TP5) also provides room for improvement. Verco can likewise improve its own security by reaching out to external service providers to conduct breach simulations and simulated attacks to test its systems (MR4).

Overall Verco has a very good commitment to adopting responsible business practices in the realm of data protection and has met the needs of the GoodCorporation Standard, with no 'non-compliance' grade in any of the 76 points in its GoodCorporation assessment.

The chart below shows the breakdown of the grades awarded to Verco, with just over half of practices working well and graded as merit or commendation.



Management and governance

Verco's senior management team has a good understanding of the importance of data protection and how to engage with the key principles underpinning effective data privacy programs. Clear policies on data protection exist (MG1), and a dedicated intranet website on data protection provides a wealth of information, including useful guidance documents and flowcharts, to employees. A very good summary of Verco's data protection policy is available online. Verco states that the comprehensive data protection policy is also available on request, but this is not clear from the website and Verco may wish to make access to its full data protection policy easier (MG3). In respect of privacy notices, Verco should redraft them to render them less legalese and more plain-English. It should also ensure that privacy notices are readily available, which is not always the case, especially in its stores (MG4).

While the data protection officer is well prepared for the role and benefits from tailored training to undertake the relevant work, just over half of the interviewed employees were not aware of who the data protection officer is. Verco may wish to communicate the role and functions of the data protection officer more pro-actively (MG5). The data protection officer's line to the board is good and works well, but data protection does not feature as a standing order agenda item during the board of director meetings – this should change (MG7). Additional help and resources for the data protection functions should be considered (MG8).

Security environment

Even though Verco's buildings' access controls are of good standards, practices in respect of locking cabinets and drawers, as well as of following the "clean-desk" policy are lacking. Several documents containing customers' personal data were left out in the open on desk tops that anyone walking by could see, and a number of drawers were left open despite also containing confidential information (PS2). Verco should ensure that it enforces the clean-desk policy and stresses the importance of locking all drawers and cabinets.

On the whole, Verco has good practices when it comes to information systems security. However, while a policy on the use of USBs, hard drives and other external devices exists, the prohibition on the use of non-Verco issued devices is not strictly enforced. Verco should consider amending its software on all laptops to ensure that only company-approved and adequately encrypted external devices can be used with Verco's laptops. In addition, it would be helpful to remind employees of the dangers of using unencrypted storage devices when transferring data (IS5). In addition, Verco should consider offering dedicated training sessions on the appropriate use of employee-owned devices including how to set up strong passwords (IS6).

In terms of dedicated IT practices, Verco should establish a formal timeline for the carrying out of independent IT assessments that cover the robustness and appropriateness of IT security controls – these should be undertaken in annual intervals, and should involve not just the IT department but also the data protection team (IS7). Training on information systems security is not consistently planned and does not form part of the official training plan for 2016 (but did for 2015), meaning that those employees who have joined Verco after 21 November 2015 have not received specific training on information systems security. Such training ideally will become a mandatory part of a new employee's induction session, and will be held in regular intervals to ensure ongoing awareness (IS8).

Legal environment

In general, the legal environment in respect of data protection and privacy at Verco is very good. There are adequate processes in place to monitor legal requirements and any relevant changes, and registrations requirements, data transfers and the handling of personal data by third parties are adequately addressed. An area for improvement is the communication of any changes to the data protection legislation to the relevant people. While changes are, on the whole, communicated clearly and speedily, and all relevant people felt they were aware of any changes, the newsletter alone may not be sufficient to communicate changes. It would be helpful to target new information more specifically to those people affected by it, by direct email contact (LE2).

Operational data practices

Verco is strong on operational data practices, with 13 out of 22 applicable practices obtaining a merit, in addition to two commendations. However, several observations and four minor non-compliance grades were also recorded.

Verco should consider changing its contracts across its operations to allow customers to immediately opt out of any information sharing not strictly necessary to the provision of the contractually agreed services. It should ensure that it does not rely, in any case, on pre-ticked consent boxes or treat silence or inaction as sufficient consent (OP1). In addition, Verco should reconsider its information gathering process. Instead of asking additional questions in the same documents as the mandatory questions (i.e. those necessary for the provision of the requested services), Verco ought to consider a separate process to ask any mandatory questions, using documents dedicated to the purpose. This would also allow it to clearly communicate the purpose of the additional information and ensure that the third party providing such information does so in a fully informed and consenting manner. In any case, Verco should ensure that it is beyond doubt what information is crucial, and what information is not strictly necessary (OP4).

At the moment, the communication of Verco's data protection policies and practices and of what the data will be used for and why at all data collection points has room for improvement. Verco should ensure that all data collection points offer the data subject to inform him or herself instantaneously about what the data is used for any it is being used in such way, without having to undertake any further research. Staff across all stores should be aware of the applicable data protection policies and practices and able to explain, at least in very broad

terms, to customers how their data is being used and why; this is not the case everywhere yet (OP5). Verco should further make sure that information related to how long data will be kept and when it will be disposed of is included in its standard customer documents (OP6).

It is commendable that Verco has devised specific policies for vulnerable groups; however, currently it is very complicated to obtain those and about 60% of the interviewees were not aware that such alternative formats even existed. The staff in Verco's stores should be trained to be able to source and distribute alternative formats in store or by mail / online. Verco should ensure that its privacy notices are adapted to the needs of children and explain the steps taken if the data subject is under 16 (OP10). In respect of obtaining explicit permission to the use of information, several customers reported that they were dissatisfied with the use of their information to send twice-monthly newsletters without explicitly asking for permission (OP12).

With regards to the monitoring of employees' use of internet, email and other communications systems, Verco has clear processes and rules. However, the enforcement system appears not to be working and additional training should be offered to line managers on how to address any inappropriate user behaviour, as well as on the importance of the appropriate use policy (OP13). For customer and data subject requests, additional training should be offered to receptionists and other customer-facing staff. Verco should ensure the reminder emails about the processes relating to data subject requests are sent regularly, and that the log book is inspected carefully by the data protection team, to guarantee that outstanding entries are dealt with in a timely manner (OP18). Finally, Verco may wish to reconsider its wide distribution of authority to disclose data, and allocate authority to disclose on a stricter basis (OP20).

Managing employees who handle data

For employees handling data, specific, job-related data protection training should be undertaken, beyond the basic overall training offered to all (ME1). Employees would also benefit from a clear and consistent communications plan, with updates on data protection issues sent not on an ad-hoc basis contingent on urgency, but in regular intervals (ME3). Currently, there is no clear disciplinary process description, and it is recommended that Verco set out in more detail what its disciplinary process entails and what the different steps are from the first formal warning letter to the ultimate sanction of dismissal. A stronger enforcement of the applicable policies would also be beneficial (ME6).

Managing routine access by third parties

As far as managing routine access by third parties is concerned, Verco should verify that the data protection policy and related standards are communicated by email in advance to each service provider or business partner, and not rely on the third party itself to request the document (TP1). Verco is aware of the importance of service providers and business partners having adequate data protection practices if they are to collect, handle or destroy data on Verco's behalf. This is demonstrated by its insistence on those other parties to provide contractually enforceable statements to that effect. However, Verco should make sure that it verifies at least some of its service providers' or business partners' data protection practices to show its own commitment and safeguard against infringements in its supply chain (TP2). In addition, Verco should consider enacting a more formal process in relation to the active management of its service providers' or business partners' handling of data and the protection thereof. It could consider asking for periodic feedback and actively engaging with its business partners or service providers in offering data protection training and checking their commitment to data protection (TP4). It should also consider including spot checks, starting with key service providers or business partners that handle large volumes of data on behalf of Verco (TP5). A verification process and such spot checks would also enable Verco to use its contractual rights to sanction where necessary (TP6).

Breaches

Verco's IT department regularly checks for internal server breaches, but Verco may wish to consider changing the times to avoid typical or repetitive behaviour. It should also ensure that reports on each check are diligently filled in and properly filed. It may also wish to consider asking for and reading the reports on the checks conducted by CloudStorage to keep an eye on its external IT systems and data storage facilities (BR1).

In respect of confidential means of reporting data protection concerns, Verco should consider revising its data protection policy to include an explicit reference to the whistleblowing hotline as being a means of reporting any data protection concerns confidentially (BR3).

Monitoring and review

While Verco appears aware of the threats emanating from the digital world, it should consider reaching out to external service providers to arrange for simulations of breaches and attacks. This should include a longer-lasting arrangement (at least 6 months), in which Verco is being tested in different ways (hacking attacks, phishing emails, spoofing, botnets, pharming and other types of common cyber security threats), and an ongoing agreement to carry out regular simulations and attacks to ensure that Verco is continuously up to speed with its data protection (MR4). Verco may also wish to consider obliging the data protection team to provide more detailed reports on a regular basis, perhaps once every six months, on any issues and information in relation to data protection and data breaches, and maintain data protection as a constant item on the agenda of each board meeting (MR5).

Action Plan

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
1.	MG3	Verco should consider publishing its complete policy on data protection on its public website, or alternatively at least make it very clear, both on the website and in the summary document provided, that the complete policy can be requested by email or by phone.	Observation				
2.	MG4	Verco should review its privacy notices and consider redrafting them in a simpler style. It should consider creating shorter summary privacy notices (of one to two pages) which highlight the most important aspects of what will happen with a data subject's information. Finally, Verco should ensure that the privacy notices are readily available online and ideally in hard copy across its stores.	Minor non-compliance				
3.	MG5	Verco should ensure that employees are pro-actively told about who the data protection officer is, e.g. by way of emails reminding them (this could form part, for example, of a "Key Contacts and Numbers" email sent out once a month and also regrouping other key contacts such as HR, whistleblowing hotlines or other important contacts), or by hanging out posters with the data protection team's details around the officer, or having info sessions dedicated to the work the data protection team does.	Observation				
4.	MG6	Verco's board should consider having data protection as a standing order agenda item at its meetings, actively inviting the data protection officer to provide a short summary or reach out to the board in advance of the board meetings, to ensure continuous exchange and reporting of data protection issues to the highest levels.	Merit				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
5.	MG7	Verco should consider holding dedicated training sessions for its senior management team to communicate the importance of data protection and ensuring that data protection is regarded as an issue that each senior manager is also responsible for. The annual meetings with the data protection team may be more useful if they were held semi-annually at least, to ensure a more up-to-date awareness among all managers.	Observation				
6.	MG8	A more streamlined process to allow the data protection team to resort to outside help if necessary, and to participate in in-depth training sessions over two or three working days would reduce the anxiety the data protection team feels about not being able to implement the latest standards of data protection. Ideally, a certain amount would be earmarked for data protection training and advice expenditure at the beginning of each year, which the data protection officer could relatively easily access.	Observation				
7.	PS2	Verco should make clear it is imperative that the clean desk policy is followed, particularly in open plan spaces and rooms which cannot be locked. One approach in enforcing this rule could be to spend some time each evening for a week or two to verify who did not abide by the clean desk policy and send the relevant people a standard email the next morning reminding them of the policy. Verco should further make it clear to employees in the head office as well as the branches that all filing cabinets and lockers must be locked by key at all times.	Minor non-compliance				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
8.	PS3	Verco should ensure that it is fully aware of the security safeguards which its off-site server providers have and ensure that its contracts spell out in detail what standards are expected. Verco may also wish to consider an updated power back-up system which last longer than only 8 hours, given that oftentimes power cuts are not addressed in that time span and forcing the internal servers to shut down may severely hamper Verco's operations (although this has not been a problem in the last ten years).	Observation				
9.	IS5	While no breach or specific incident has been reported, Verco should consider amending its software on all laptops to ensure that only company-approved and adequately encrypted external devices can be used with those laptops. In additional, Verco should ensure that all its staff are aware of the policy on the use of external devices and realise the inherent dangers in using personal external devices, especially non-encrypted ones, when accessing, transferring or storing data.	Minor non-compliance				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
10.	IS6	Verco's policy includes examples of best practices including of how to create strong passwords, but this is not widely known among employees. Verco should consider offering dedicated training sessions on the appropriate use of employee-owned devices. For instance, before an employee is granted access to work email on his or her phone, the IT team could send across a detailed summary of how to use the device and how to create passwords, as well as the need to register the device and record its serial number.	Observation				
11.	IS7	Verco should establish a formal timeline for the carrying out of independent IT assessments that cover the robustness and appropriateness of IT security controls – these should be undertaken at least annually. In addition, this should not just be the purvey of the IT department, but actively involve the data protection team as well.	Observation				
12.	IS8	Verco should consider making such training mandatory part of a new employee's induction session, and hold such training in regular annual intervals to refresh employees' awareness.	Minor non-compliance				
13.	LE2	In addition to the weekly newsletter, it is helpful to target new information more specifically to those people who will be responsible for it. For instance, a change in the IT requirements should always also be specifically mentioned and sent to the IT department separately.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
14.	OP1	Verco should change its contracts, both online and in hard copy, to allow customers to immediately opt out of any information sharing not strictly necessary to the provision of services. Ideally, customers would have to explicitly opt in before giving any such consent. Verco should make sure that all customers are fully informed of their rights in relation to consent, whether they enter into a contract online or in a store. It is noted that the law in relation to consent is strengthened from May 2018 onwards - consent under the GDPR requires clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute clear affirmative action. Verco must consider this and revise its standard approach to obtaining consent in time to comply with the GDPR.	Minor non-compliance				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
15.	OP4	Verco should reconsider its information-gathering process. Instead of asking additional questions in the same documents as the mandatory questions (i.e. those necessary for the provision of the requested services), Verco could have a separate process to ask any mandatory questions, on a different set of paper. This would also allow it to clearly communicate the purpose of the additional information and ensure that the third party providing such information does so in a fully informed and consenting manner. In any case, Verco should ensure that it is beyond doubt what information is crucial, and what information is not strictly necessary. In addition, Verco should ensure it has a clear idea for what it intends to use any information obtained, and why it is asking certain questions. This will allow it to communicate the statement of purpose before asking the relevant questions, and does not facilitate the risk of asking as many questions as possible and considering what to do with the answers afterwards.	Minor non-compliance				
16.	OP5	Verco should ensure that all data collection points offer the data subject to inform him or herself instantaneously about what the data is used for and why it is being used in such way, without having to click on other websites and undertake additional research. Verco should also make sure that its staff are universally aware of the applicable data protection policies and practices and able to explain, at least in very broad terms, to customers how their data is being used and why, where relevant.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
17.	OP6	Third parties as well as staff should be able to have a quick sense of what happens to their data if it is being disposed of and what the timeframe for keeping such data is. Verco should consider including that information in the standard documents and contracts in the section on data protection and privacy.	Observation				
18.	OP7	See OP1.	Observation				
19.	OP10	The staff in Verco's stores should be trained to be able to source and distribute alternative formats of the privacy notices without any delay. Ideally, they would be able to directly distribute such alternative formats in store or by mail / online without having to first contact Verco's head office. Verco should ensure that its privacy notices are adapted to the needs of children and explain the steps taken if the data subject is under 16.	Minor non-compliance				
20.	OP12	Verco should ensure that those uses which would, by most customers at least, be deemed to go beyond the strictly necessary to enable the provision of services are highlighted and require specific permission.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
21.	OP13	Verco should consider offering training sessions to line manager on how to address inappropriate user behaviour, and stress the importance of following the appropriate use policy. In addition, Verco may wish to consider a blanket ban on the use of personal laptops and hand held devices / other internet-connected devices during office hours, and re-circulate its communication about what may and what may not be accessed or circulated by employees during office hours or using office equipment.	Observation				
22.	OP14	A clear guideline how often and in what intervals the data subject should be reminded to respond after the initial email should be implemented and shared among all relevant employees.	Merit				
23.	OP18	Training for receptionists and anyone who is customer-facing should include a dedicated section on how to deal with data subject requests. It may also be helpful to send out regular reminder emails (once a month) to highlight the relevant policies and where to access them. The data protection team should ensure that the log book is inspected carefully on a regular basis (at least once to twice a week) and that any outstanding entries are dealt with as soon as reasonably practicable.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
24.	OP19	Verco should not use categories to allow general authority to employees, but should allocated authority on strict basis of necessity and consider the duties and job description of each employee before giving the employee data sharing authority.	Observation				
25.	OP23	Verco should update its policies to clearly include genetic and biometric data as sensitive data.	Merit				
26.	ME1	Verco should tailor specific training according to an employee's needs. Basic overall training is a good idea, but additional training should be considered for those who are likely to have to deal with requests, process large amounts of personal data (HR staff members, customer-facing employees) etc.	Observation				
27.	ME3	Verco should consider spending some time setting up a clear communications plan with respect to data protection issues, responding not only to specific topics or matters of urgency, but also ensuring that data protection reminders are sent in regular intervals, with links and information for employees to refresh their knowledge and raise overall awareness.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
28.	ME6	Verco should set out in more detail what its disciplinary process entails and what the different steps are from the first formal warning letter to the ultimate sanction of dismissal. This should be contained in an updated Code of Conduct. Verco should further ensure that the formal disciplinary process is actually used in respect of data protection infringements to signal that it is serious about the respect of its data protection policies. A formal first warning letter to employees in breach of a data protection rule, setting out what the infringement is, how to avoid such infringement and offering to discuss and/or provide further clarification in person would be a good first step. In addition, Verco may wish to consider including a sample (fictitious or anonymised) case study in its Code of Conduct or its data protection policy on how the disciplinary process would be used in respect of infringements of the organisation's data protection rules.	Minor non-compliance				
29.	TP1	Verco should ensure that the data protection policy and related standards are communicated by email in advance in each case, and not rely on the third party to obtain the documents itself instead.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
30.	TP2	Verco is aware of the importance of service providers and business partners having adequate data protection practices if they are to collect, handle or destroy data on Verco's behalf. This is demonstrated by its insistence on those other parties to provide contractually enforceable guarantees to that effect. However, Verco should make sure that it verifies at least some of its service providers' or business partners' data protection practices to show its own commitment and safeguard against infringements in its supply chain.	Minor non-compliance				
31.	TP4	Verco should consider enacting a more formal process in relation to the active management of its service providers' or business partners' handling of data and the protection thereof. It could consider asking for periodic feedback and actively engaging with its business partners or service providers in offering data protection training and checking their commitment to data protection.	Observation				
32.	TP5	Verco should include spot checks, starting with key service providers or business partners that handle large volumes of data on behalf of Verco	Minor non-compliance				
33.	TP6	While there is no suggestion that service providers or business partners have in fact failed to meet Verco's required standards for data protection, Verco should strongly consider (as set out in TP2 and TP4) a verification process and spot checks to ensure compliance, and enable it to use its contractual rights to sanction where necessary.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
34.	BR1	Verco may wish to consider changing the times when it checks for data breaches to avoid any repetitive or typical behaviour. It should further ensure that the reports on each check are diligently filled in and properly filed. Finally, it may wish to consider asking for and reading the reports on the checks conducted by CloudStorage to keep an eye on its external IT systems and data storage facilities.	Observation				
35.	BR3	Verco should consider revising its data protection policy to include an explicit reference to the whistleblowing hotline as being a means of reporting any data protection concerns confidentially. It would also be helpful to add that information to the induction training and make it as well known as the identity of those the staff should speak to if they have any queries.	Observation				
36.	MR2	Verco may wish to consider including the effectiveness of existing data protection measures as a standing order agenda item at board meetings.	Observation				

No.	Framework point	Recommendation(s)	Grade	Verco's comments (if any)	Action to be taken by Verco	Owner	Timeframe
37.	MR4	Verco should consider reaching out to external service providers to arrange for simulations of breaches and attacks. This should include a longer-lasting arrangement (at least 6 months), in which Verco is being tested in different ways (hacking attacks, phishing emails, spoofing, botnets, pharming and other types of common cyber security threats), and an ongoing agreement to carry out regular simulations and attacks to ensure that Verco is continuously up to speed with its data protection.	Minor non-compliance				
38.	MR5	As mentioned in MG6, data protection should become a standing order agenda item at each board meeting. In addition, Verco may wish to consider obliging the data protection team to provide a more detailed report, perhaps once every six months, on any issues and information in relation to data protection and data breaches.	Observation				

Appendix 1 Detailed findings

1. Management and governance

MG1: There is a written and clearly articulated policy on data protection, which is referred to in the organisation's code of conduct.	Grade: Commendation
Verco has a written and clearly articulated policy on data protection. This is referred to in Verco's Code of Conduct, and is clearly signposted on the homepage of the organisation's intranet. A summary of the data protection policy is made available on Verco's publicly accessible homepage.	
Assessment:	
The policy on data protection captures a variety of issues and clearly sets out the rights and obligations of all staff and the policy on employee'-owned devices. It also contains a section on addressing the needs of vulnerable members of staff or customers, including children. The policy appears in an easy-to-use format, and across interviews employees were confident that a policy existed, where to find it, and how to use it. There was clear ownership and version control, with the last version having been updated in July 2016 in preparation for the legislative changes coming into force with the start of the EU General Data Protection Regulation (**GDPR**) in 2018.	

MG2: The policy and the measures in place have been formally approved by the board.	Grade: Merit
The revised version of the data protection policy has been signed off formally at Verco's latest company board meeting on 29 July 2016.	
Assessment:	
While the latest version was a dedicated minute on the agenda of July's board meeting, the previous two versions had not been formally approved by the board. The reason given was that the two previous updates (in February 2015 and April 2014) concerned mostly typographical updates and did not touch on any substantive content.	
Recommendations:	
It is advisable to ensure that each update of the data protection policy, as well as any processes in connection with the data protection policy, is formally approved by the board. Making sure that data protection becomes a standard point on the agenda of each board meeting is a recommended way to guarantee that anything in relation to data protection is regularly and continuously considered by the board.	

MG3: Both the complete policy and a summary of the policy are made public.	Grade: Observation
A summary of the data protection policy is made available on Verco's publicly accessible homepage. The complete policy is not available publicly.	
Assessment:	
The summary of the data protection policy is well presented and captures the key points of the long-form policy. However, for members of the public without access to Verco's intranet, there is no easy way to obtain the comprehensive policy – the data protection officer made it clear that the complete policy can be made available on request, but this is not obvious from visiting Verco's website and not formally written down anywhere easily accessible.	
Recommendation:	
Verco should consider publishing its complete policy on data protection on its public website, or alternatively at least make it very clear, both on the website and in the summary document provided, that the complete policy can be requested by email or by phone.	

MG4: The organisation has readily accessible privacy notices in place which include the legal basis for processing data, data retention periods and a data subject's right to complain and to whom. The information provided in the privacy notice is given in a clear, concise and easy to understand language.	Grade: Minor non-compliance
The website contains a comprehensive privacy note which sets out the way in which the information gathered from the website visitor and/or online customer is being used and meets the legal requirements. In stores, privacy notices form part of the contractual documents or are referred to.	
Assessment:	
The privacy notices are written in a complicated and legalistic style. A big majority of interviewed customers and suppliers (more than 75%) found the privacy notices to be unclear, lengthy and difficult to understand. In stores, while privacy notices or references to privacy notices form part of any paper work and contractual documents which customers may enter into, these are not readily accessible. Staff often did not know how to locate the full privacy notice (despite references in the paperwork to reach out to staff to obtain the full privacy notices), and in half of the surveyed stores, no hard copies of the privacy notices were available.	
Recommendations:	
Verco should review its privacy notices and consider redrafting them in a simpler style. It should consider creating shorter summary privacy notices (of one to two pages) which highlight the most important aspects	

of what will happen with a data subject's information. Finally, Verco should ensure that the privacy notices are readily available online and ideally in hard copy across its stores.

MG5: There is a named person responsible for data protection who is made known to employees and signposted as a source of guidance on data protection queries.	Grade: Observation

Verco's data protection officer is Miguel Samarrco, who heads a dedicated data protection team of three people. His name and the existence of the data protection team is mentioned in the Verco's and the Group's data protection policy, and made it clear on Verco's intranet website in the data protection section.

Assessment:

While it is clear who is responsible for data protection, just over half of the employees interviewed did not know who the data protection officer was, or how to find out who to talk to if they needed guidance on data protection queries.

Other than the communication on the policies and intranet, there was no effort to inform employees of the data protection team. One email was sent out at Miguel Samarrco's appointment to the role as data protection officer in January 2014, but not further direct communication appears to have been undertaken since then.

Recommendations:

Verco should ensure that employees are pro-actively told about who the data protection officer is, e.g. by way of emails reminding them (this could form part, for example, of a "Key Contacts and Numbers" email sent out once a month and also regrouping other key contacts such as HR, whistleblowing hotlines or other important contacts), or by hanging out posters with the data protection team's details around the officer, or having info sessions dedicated to the work the data protection team does.

MG6: The responsible person has a reporting line to the board.	Grade: Merit

The data protection officer (currently Miguel Samarrco) has a direct reporting line to the board.

Assessment:

It is possible for the data protection officer to reach out directly to the board should he wish so. He is however not a regular participant in the board meetings and has contact with the board only on his own initiative.

Recommendations:
Verco's board should consider having data protection as a standing order agenda item at its meetings, actively inviting the data protection officer to provide a short summary or reach out to the board in advance of the board meetings, to ensure continuous exchange and reporting of data protection issues to the highest levels.

MG7: Senior management champions and sets the tone on data protection.	Grade: Observation
Verco's senior management usually know who the data protection officer is and annual meetings bring together all of the senior management and the data protection team to discuss development over the last year and challenges ahead.	
Assessment:	
While most senior managers were aware of the data protection team and would circulate information from the team amongst their own departments, there was a lack of pro-active engagement with the data protection team. A mentality that data protection is not part of their responsibility and should be left to the experts and the lawyers appears to pervade most of senior management.	
Recommendations:	
Verco should consider holding dedicated training sessions for its senior management team to communicate the importance of data protection and ensuring that data protection is regarded as an issue that each senior manager is also responsible for. The annual meetings with the data protection team may be more useful if they were held semi-annually at least, to ensure a more up-to-date awareness among all managers.	

MG8: Adequate resources are devoted to implementing and monitoring data protection.	Grade: Observation
Verco's data protection team consists of three people who are working full time on keeping up-to-date with legal developments and devise the policies and training programmes for Verco's operations across the country. For each of Verco's branches, an employee is nominated responsible for data protection issues and specifically trained by Verco's data protection team.	
Assessment:	
Overall, there is sufficient support and resources devoted to the data protection team and its work in implementing and monitoring data protection. However, it is very difficult – and takes up to two months – to obtain permission to engage outside services for specific data protection projects, such as comprehensive training courses or additional legal advice and guidance by private law firms. This results in a general concern that it is difficult ensuring that all data protection team are aware of the latest legal updates, and able to	

comprehensively consider all aspects of data protection. In addition, there are certain "crunch times" when outside help and advice is considered indispensable. To obtain permission for funding to engage, for example, an outside law firm, takes a considerable amount of time (in the context of the GDPR and specific questions as to how it would impact the telecommunications sector, the data protection team had to wait for two months before it got permission to engage a data protection lawyer for a total of 10 billable hours).
Recommendations:
A more streamlined process to allow the data protection team to resort to outside help if necessary, and to participate in in-depth training sessions over two or three working days would reduce the anxiety the data protection team feels about not being able to implement the latest standards of data protection. Ideally, a certain amount would be earmarked for data protection training and advice expenditure at the beginning of each year, which the data protection officer could relatively easily access.

2. Risk Assessment

RA1: Regular risk assessments consider data protection risks and impacts on privacy, and the effectiveness of mitigation measures, both within the organisation and in association with third parties. Assessments are conducted at least annually.	Grade: Commendation
Verco conducts its risk assessments in relation to data protection risks and impacts on privacy on a very regular basis, with a dedicated meeting every three months. In addition, each department at Verco must consider data protection risks and impacts on privacy in any new project they engage in, by filling in a paper document and acknowledging that data protection risks are either acceptable or mitigated.	
Assessment:	
Verco's approach to risks assessments is exemplary, and forms an integral part of its business conduct.	

RA2: Data protection and privacy are considered by design and by default in respect of any new activities and products, including privacy impact assessments where necessary.	Grade: Merit
Each department must conduct a data protection risk assessment before engaging in any new project.	
Assessment:	
The risk assessments form part of the day-to-day business conduct and data protection and privacy are considered by design and by default. A revised risk assessment paragraph has been issued after the publication of the new GDPR, and explicit references are made to consideration by design and by default in Verco's code of conduct and risk assessment guidelines.	

3. Security Environment

Physical Security

PS1: Buildings where data is stored are properly secured with controlled access.	Grade: Merit
To access Verco's offices, a touch key is required which is issued only to employees of Verco. The IT and archive rooms have extra locks which only a handful of employees have keys to. In stores, access is generally secured by lockable doors and a metal gate which is closed overnight. The offices and all stores are alarmed, which is turned on and off by code. This code is on average changed every three months. All visitors must register before accessing Verco's head office and must be accompanied by a member of staff at all times.	
Assessment:	
The access controls Verco employs are of a good standard.	

PS2: Hard copy files and servers are kept in locked rooms, cabinets or storage facilities with controlled access.	Grade: Minor non-compliance
All cabinets and storage facilities in Verco's offices and in the branches can be locked. Servers, to the extent these are on-site, are in separate rooms and can be accessed only by a specifically authorised IT employees with special key cards. An electronic system records the time of any access and whose key card is used. CCTV operates in the server rooms.	
Assessment:	
It is Verco's policy to keep all hard copy files under lock and key. It is also official policy for every employee to have a "clean desk" at the end of each working day, i.e. to lock away any files in the employee's cabinet or securely store them elsewhere. However, some of the lockers and cabinets were not, in fact, locked when the assessors tried to open them. In almost a third of the stores, the store managers and employees did not bother locking their cabinets. A significant number of the employees in Verco's head office did not abide by the clean desk policy, and several documents containing customers' personal data were left out in the open for anyone walking by to see.	
Recommendations:	
Verco should make clear it is imperative that the clean desk policy is followed, particularly in open plan spaces and rooms which cannot be locked. One approach in enforcing this rule could be to spend some time each evening for a week or two to verify who did not abide by the clean desk policy and send the relevant people a standard email the next morning reminding them of the policy. Verco should further make it clear to employees in the head office as well as the branches that all filing cabinets and lockers must be locked by key at all times.	

PS3: There is protection for equipment containing data from environmental hazards including fire, flood and power failure.	Grade: Observation
Verco's main servers are off-site and operated by one of the UK's biggest cloud and server company, CloudStorage Ltd. Verco's offices and each branch has fire extinguishers for all types of fires, and there is an extremely low flooding risk in any of Verco's sites. All employees use laptops for work. A back-up battery system lasting about 8 hours supports the internal servers at Verco's head office should there be a power cut, but apart from that there is no separate power generation if power fails.	
Assessment:	
While no specific dangers have been identified, and no incidents have ever been reported, there was a general lack of awareness of how the equipment on Verco's sites is protected against fire, flood or power failures. With regards to the off-site servers, it was trusted that CloudStorage would have sufficient safeguards against environmental hazards, but there was no knowledge of what such safeguards actually consisted in. This was not specifically addressed in the service contract between CloudStorage and Verco, but does form part of the overall terms and conditions that CloudStorage applies to all of its contracts.	
Recommendations:	
Verco should ensure that it is fully aware of the security safeguards which its off-site server providers have and ensure that its contracts spell out in detail what standards are expected. Verco may also wish to consider an updated power back-up system which last longer than only 8 hours, given that oftentimes power cuts are not addressed in that time span and forcing the internal servers to shut down may severely hamper Verco's operations (although this has not been a problem in the last ten years).	

Information Systems Security

IS1: Access to electronic data is regulated by user identification and authentication.	Grade: Merit
Each laptop and each access to any of Verco's intranet sites are user authenticated and password protected. Electronic information is accessible according to a "need to know" basis.	
Assessment:	
Verco employs a good standard of identification and authentication, with electronic data being accessible only to those people who are authorised to access it (e.g. only certain people in HR have access to staff records). Passwords must be changed every 60 days and require a combination of letters, numbers and special symbols.	

IS2: Data access controls (including read, write, amend, move, copy and delete privileges) and, where necessary, security levels are in place and regularly reviewed.	Grade: Merit
Data access controls are in place across Verco's systems, with different level of confidentiality for different sets of documents.	
Assessment:	
Verco has a thorough system of data access controls and ensures that any access privileges correspond to the function and role of the relevant employee. Documents of higher confidentiality will not be visible, let alone accessible, to those employees not cleared to access such confidentiality levels.	

IS3: Changes to the systems that store and process data are properly controlled and subject to segregation of duties.	Grade: Merit
The IT department is responsible for the systems that store and process data and ensures that all changes are made appropriately.	
Assessment:	
Any changes to the systems can only be made by the IT department, but must be signed off by senior management. Once a change is envisaged, the senior manager receives an email inviting him to electronically authorise the change – only once this has been authorised, can the change be made.	

IS4: Laptops, smart phones and other portable devices are encrypted and if appropriate have remote memory wipe facility.	Grade: Merit
Laptops and any portable devices issued by Verco to its employees are all encrypted, and have remote memory wipe facility.	
Assessment:	
Verco employs a system of electronic registration of all its devices and is able to access them to remote wipe their memory if necessary. The default setting on most devices is that once the password is entered incorrectly more than three times, the device will lock itself and can be unlocked only by a member of Verco's IT security team.	

IS5: There is a policy on the use of USBs, hard drives and other external devices.	Grade: Minor non-compliance
Verco does have a policy on the use of USBs, hard drive and other external devices. Non-Verco issued external devices are prohibited and only encrypted external devices can be used.	
Assessment:	
While a policy exists, it is not strongly enforced. Verco is conscious of the dangers that the use of non-encrypted external devices present, but a number of employees have reported that they frequently use their own USB devices to transfer data containing personal data. The Verco issued-laptops are usually still compatible with external devices not issued by Verco, and for reasons of time and convenience employees are tempted to ignore the policy on the use of external devices. No breach has ever been reported and all employees bar one reported that they would securely delete the data from their external device as soon as the transfer was completed or it was no longer necessary to store it.	
Recommendations:	
While no breach or specific incident has been reported, Verco should consider amending its software on all laptops to ensure that only company-approved and adequately encrypted external devices can be used with those laptops. In additional, Verco should ensure that all its staff are aware of the policy on the use of external devices and realise the inherent dangers in using personal external devices, especially non-encrypted ones, when accessing, transferring or storing data.	

IS6: There is a policy on the use of private and/or employee-owned devices.	Grade: Observation
The employment handbook contains a dedicated section on the use of employee-owned devices and sets out examples of best practices as well as minimum safety requirements (namely the need to register and password protect the device).	
Assessment:	
Not all employees knew whether their device (usually mobile phones, but in some cases also iPads and similar electronic devices) was registered and the serial number recorded. All interviewees who used their own devices (usually for work email) used passwords, but not all were confident if their passwords were strong passwords and did not always know how to devise strong passwords. Before access to work email is granted, the IT department must send an authentication key to the employee's device.	
Recommendations:	
Verco's policy includes examples of best practices including of how to create strong passwords, but this is not widely known among employees. Verco should consider offering dedicated training sessions on the	

appropriate use of employee-owned devices. For instance, before an employee is granted access to work email on his or her phone, the IT team could send across a detailed summary of how to use the device and how to create passwords, as well as the need to register the device and record its serial number.

IS7: There is independent testing of the robustness and appropriateness of the IT security controls and the person responsible for data protection is informed of the results.	Grade: Observation
Verco conducted an IT audit for the last time in 2013. This assessment included information systems and overall security control.	
Assessment:	
The IT department is considered responsible for organising the testing of the robustness and appropriateness of the IT security controls. The data protection team was only vaguely aware of the last IT assessment and did not know how to access it without going through the IT department. There is as yet no formal process in place to establish the frequency of independent IT assessments, but one has been mentioned for early 2017.	
Recommendations:	
Verco should establish a formal timeline for the carrying out of independent IT assessments that cover the robustness and appropriateness of IT security controls – these should be undertaken at least annually. In addition, this should not just be the purvey of the IT department, but actively involve the data protection team as well.	

IS8: Specific training on information systems security is organised for all employees.	Grade: Minor non-compliance
Specific training on information systems security formed part of the training plan 2015 but does not form part of the training plan of 2016.	
Assessment:	
Any employee in either the head office or the branch who started after the 21 November 2015 has not received specific training on information systems security.	
Recommendations:	
Verco should consider making such training mandatory part of a new employee's induction session, and hold such training in regular annual intervals to refresh employees' awareness.	

4. Legal environment

LE1: There is a process to monitor and comply with the applicable legal requirements in all the jurisdictions in which the organisation handles data or where liability might arise.	Grade: Merit
The data protection team, composed entirely of qualified lawyers, follows the development in data protection law and monitors all legal requirements.	
Assessment:	
It is clear who is responsible for monitoring and ensuring that Verco complies with the applicable legal requirements. The data protection team cooperates well with the legal team. Regular meetings, about once every two to three weeks, are held between the data protection team and the legal team to monitor developments in the world of data protection and privacy.	
Recommendations:	
While the legal teams at Verco monitor any developments, Verco may wish to consider to make it easier for its legal staff to attend comprehensive training sessions conducted outside the firm (see MG8).	

LE2: Changes to the applicable data protection legislation are communicated clearly and speedily to the relevant people within the organisation. The impact of any changes on the organisation's policies and processes is constantly evaluated.	Grade: Observation
Any changes to the applicable data protection legislation are summarised in a weekly newsletter that is sent around the company. The legal meetings (see LE1) cover the impact of any changes on Verco's policies and processes.	
Assessment:	
See LE2 – changes are generally communicated clearly and speedily, and all relevant people felt they were aware of any changes in a timely manner. However, Verco should ensure that information is specifically targeted to those people who will be concerned by it - there is a risk that the newsletter will not be read by employees (about 20% interviewees reported that they would delete or file the newsletter immediately without reading it in full).	
Recommendations:	
In addition to the weekly newsletter, it is helpful to target new information more specifically to those people who will be responsible for it. For instance, a change in the IT requirements should always also be specifically mentioned and sent to the IT department separately.	

LE3: Where legally required, the organisation has registered with the appropriate data protection authorities in the different jurisdictions in which it operates.	Grade: Merit
Verco is registered with the Information Commissioner's Officer (**ICO**).	
Assessment:	
The registration with the ICO was complete and up-to-date.	

LE4: The legal implications of any data transfers, including cross-border data transfers, have been considered, and there is a system in place to ensure that data transfers do not compromise the adequate protection of personal data.	Grade: Merit
As a telecommunications provider, Verco's data flows inevitably across multiple boundaries. The data protection team and the legal team consider cross-border transfer at their regular meetings. Verco's flowchart "International Transfers" (available on the firm's intranet) sets out in detail the location of servers and data hubs and covers the necessary steps to take and verify in relation to international data transfers.	
Assessment:	
The adequate protection of personal data is considered in-depth by Verco in relation to international transfers. The legal team and data protection team have included model clauses in all of their international contracts. It conducts regular risk assessment on whether the data transfers outside the UK are provided with an adequate level of protection for the rights of the data subjects, and a list of potential steps is available to take should the level not be deemed adequate.	

LE5: Where any third parties handle data on the organisation's behalf, the legal implications of this have been considered and the obligations for each relevant party are clearly set out in a contractual manner.	Grade: Merit
All contracts with third party have a dedicated data protection and privacy section and clearly set out the obligations and rights of both parties, as well establishing precisely who assumes the role of data controller and data processor.	
Assessment:	
The contractual framework that Verco enters into with any third party that handles personal data on its behalf are clear and comprehensive. They include provisions to terminate and/or demand substantial damages for any breach of the data protection clauses, and any breach has serious contractual consequences. The	

preamble of each contract mentions the importance of adequate data protection and of abiding by the provisions related to it.

5. Operational data practices

OP1: The organisation obtains subjects' free, specific, informed and unambiguous consent prior to gathering data.	Grade: Minor non-compliance

Each of the contracts surveyed that recorded any type of personal data has provisions governing the issue of consent. Verco's website has a pop-up window explaining the cookies employed and info gathered.

Assessment:

Internally, Verco's contracts are clear and ask for specific consent of its employees prior to gathering any data on them. On its website, it is impossible to access the main page without first agreeing to the notification that appears immediately upon visiting www.vercotelecom.co.uk.

Verco also enters into many contracts a day with customers across the country both online and in its stores. The contract it employs when customers are, for instance, setting up a new mobile phone payment plan, includes consent language which is fairly wide in its language. It is impossible to opt out of marketing emails and the sharing of data with third parties other than by writing a separate letter to Verco's head office. Once received, the relevant person will be notified and the name removed from any marketing list and data sharing list within 24 hours.

The consent language forms part of the overall small print in Verco's standard contracts, in the data protection and information sharing section. There is no separate summary nor is the consent language highlighted in any particular way. Staff training in stores includes verbally reminding the customer of the consent language and that he or she, by signing, agrees for his or her data to be used; some stores offer to immediately remove the names from any marketing or information sharing lists if the customers so wishes, without the customer having to go through sending a letter. However, there is no uniform approach, and not all staff members remembered that they should remind customers of the information sharing the customers agree to by signing the contract. Several customers interviewed were unaware of their opt-out rights and uncertain whether they had to provide consent or not, or whether they could withdraw consent once given.

Any changes to the terms and conditions in relation to privacy are well communicated and clearly set out. Customers are emailed and sent a letter setting out the changes, and offering an immediate opt-out, or indeed termination of the contract without any cancellation fees, by clicking a link (in the email) or by calling a number (both in the email and in the letter).

Recommendations:

Verco should change its contracts, both online and in hard copy, to allow customers to immediately opt out of any information sharing not strictly necessary to the provision of services. Ideally, customers would have to explicitly opt in before giving any such consent. Verco should make sure that all customers are fully informed of their rights in relation to consent, whether they enter into a contract online or in a store.

It is noted that the law in relation to consent is strengthened from May 2018 onwards - consent under the GDPR requires clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute clear

affirmative action. Verco must consider this and revise its standard approach to obtaining consent in time to comply with the GDPR.

OP2: The organisation has systems in place to ensure the recording of any consent given and the existence of an effective audit trail.	Grade: Merit
A complex filing management system has the records of all customers and other third parties, and offers specific search functions in relation to whether any individual third party has consented, how they consented, and to what they consented.	
Assessment:	
Verco appears to have a robust filing system and organises its records very well, giving rise to the existence of an effective audit trail.	

OP3: If the organisation buys data, it ensures that data subjects have consented to the use to which the data is being put.	Grade: Not applicable
Verco does not buy any data.	

OP4: The organisation collects only such information that it requires for its stated purpose, and strives to minimise any data collection to that which is strictly necessary.	Grade: Minor non-compliance
The information Verco collects covers people's names, addresses, bank details, birthdays, personal password questions which include, amongst other options, a person's mother's maiden name, the names of any children or other personal information. In addition, Verco offers non-mandatory questions relating to a person's hobbies, interests and frequently visited locations, in order to "optimise any information shared with" a customer.	
Assessment:	
Verco makes the provision of information mandatory only to the extent this is required to provide its services to a third party. However, it asks additional questions, which, although not mandatory, serve to obtain additional personal information and are not strictly necessary. Not all customers were aware that some of the information requested was not, in fact, mandatory to give.	

Recommendations:
Verco should reconsider its information-gathering process. Instead of asking additional questions in the same documents as the mandatory questions (i.e. those necessary for the provision of the requested services), Verco could have a separate process to ask any mandatory questions, on a different set of paper. This would also allow it to clearly communicate the purpose of the additional information and ensure that the third party providing such information does so in a fully informed and consenting manner. In any case, Verco should ensure that it is beyond doubt what information is crucial, and what information is not strictly necessary. In addition, Verco should ensure it has a clear idea for what it intends to use any information obtained, and why it is asking certain questions. This will allow it to communicate the statement of purpose before asking the relevant questions, and does not facilitate the risk of asking as many questions as possible and considering what to do with the answers afterwards.

OP5: The organisation communicates its data protection policies and practices and what it will use the data for and why, at all data collection points.	Grade: Observation
Many of Verco's data protection policies and practices are available online, and contracts generally state what it will use the data for and why.	
Assessment:	
While all data collection points usually have a document or at least a statement available to the data subject explaining what Verco's data protection policies and practices are, some of them merely refer to where the data protection policies and practices can be found, and make it unduly complicated to find out what the data will be used for and why. Customer-facing staff generally had a good sense of what the data will be used for and why, and were able to communicate this to customers. However, some of the staff were uncertain and would not feel confident explaining to third parties the use of the data and why it is being collected.	
Recommendations:	
Verco should ensure that all data collection points offer the data subject to inform him or herself instantaneously about what the data is used for and why it is being used in such way, without having to click on other websites and undertake additional research. Verco should also make sure that its staff are universally aware of the applicable data protection policies and practices and able to explain, at least in very broad terms, to customers how their data is being used and why, where relevant.	

OP6: The organisation communicates its policy on how long it will keep data and how it will dispose of it.	Grade: Observation
How long data is kept and how it will be disposed of is contained in the summarised data protection policy.	
Assessment:	
The summary of the data protection policy is available publicly on Verco's website, however, most standard documents and contracts do not specify how long Verco will keep the collected data and how it will be disposed of. A significant majority (74%) of interviewed staff and third parties did not have any idea of how long their data is likely to be kept and how it will be disposed of.	
Recommendations:	
Third parties as well as staff should be able to have a quick sense of what happens to their data if it is being disposed of and what the timeframe for keeping such data is. Verco should consider including that information in the standard documents and contracts in the section on data protection and privacy.	

OP7: The organisation obtains subjects' consent prior to disclosing or selling their data to third parties and explains the purpose of the disclosure.	Grade: Observation
Consent is obtained through contractual documents and other documents which require a data subject's signature.	
Assessment:	
While Verco has valid consent for the data to be disclosed (it does not sell any data) to third parties, it is not always clear that this consent was given explicitly and unambiguously. Some of the consent is obtained implicitly by signing a contract of whatever nature with Verco, and can be revoked only by reaching out directly to Verco (see OP1).	
Recommendations:	
See OP1.	

OP8: The organisation makes reasonable efforts to explain to vulnerable people their rights and to guide them on sensible precautions they can take to protect their data.	Grade: Commendation

At least one staff member in each of Verco's stores has undergone a dedicated half-day training course in dealing and engaging with vulnerable people, which includes a section on protection their data and talking to the subjects about what precautions can be taken. Verco issues specific guidelines of engaging with vulnerable people, which include a section on data protection. All staff obtain a copy of the guidelines, and frontline staff must do an annual online training session on the guidelines.
Assessment:
Verco's guidelines are clear and comprehensive, and include sections on, *inter alia*, identifying vulnerable customers, practical tips on how to engage with them, specific considerations for frontline staff, and guidance on how their personal data should be protected.

OP9: The organisation has systems in place to verify data subjects' ages and to obtain parental or guardian consent for any data processing where necessary.	Grade: Merit
For any contract, a proof of age must be provided in form of a passport or driving licences, together with a second form of identity such as a bank card or utility statement.	
Assessment:	
Verco has specific guidelines in place of how to deal with anyone below 18 and below 16, in accordance with the applicable laws. For under-16s, generally consent is required from parents or legal guardians.	

OP10: Privacy notices are adapted to the needs of children or other vulnerable individuals where their data is being processed.	Grade: Minor non-compliance
The privacy notices contain a note stating that there are also available in other forms (including braille, large type-set and audio version). No specific privacy notice exists adapted to the needs of children.	
Assessment:	
It is very positive that alternative formats of the privacy notice are available. However, to obtain a privacy notice in a format other than the standard one which is available online, it is necessary to write an email / call Verco specifically, and it may take up to a week before it is provided. About 60% of the interviewees were not aware that alternative formats existed, and were unsure how to obtain them.	

Recommendations:
The staff in Verco's stores should be trained to be able to source and distribute alternative formats of the privacy notices without any delay. Ideally, they would be able to directly distribute such alternative formats in store or by mail / online without having to first contact Verco's head office. Verco should ensure that its privacy notices are adapted to the needs of children and explain the steps taken if the data subject is under 16.

OP11: There is a policy on the use of CCTV and audio recording which is made available to all those who could be recorded.	Grade: Merit
The policy on the use of CCTV and audio recording is contained within the overall data protection policy and is also referred to in the privacy notices.	
Assessment:	
CCTV and audio recordings, while employed very sparingly by Verco, are mentioned in the relevant policies which can be easily accessed by those who could be recorded.	

OP12: Information collected is used only in the ways for which the organisation has explicit permission.	Grade: Observation
Information on the use of the collected data can be accessed by the data subjects before their data is collected, and the contractual documents contain provisions which by signing give permission to use the collected information as intended.	
Assessment:	
By entering into any sort of contract the data subjects give their permission for their data to be used in accordance with Verco's standard policies and processes. However, not all customers confirmed that they had given explicit permission for some uses, such as sending a twice monthly newsletter to Verco's customer informing them of special deals and promotions. Even though legally, permission was clearly given, many customers did not feel that explicit permission was given to use their data in ways that go beyond the merely operational and necessary to satisfy a customer's service requirements.	
Recommendations:	
Verco should ensure that those uses which would, by most customers at least, be deemed to go beyond the strictly necessary to enable the provision of services are highlighted and require specific permission.	

OP13: There are processes which govern the monitoring of employees' use of internet, email and other communications systems.	Grade: Minor non-compliance
Verco's internal employment handbook sets out the rules and regulations pertaining to employees; use of internet, email and other communications systems. All use is entitled to be monitored and a records log may be kept of any use.	
Assessment:	
The employment handbook clearly sets out the processes governing the monitoring of employees' use of internet, email and other communications systems. Certain use is entirely prohibited, such as accessing pornographic material or accessing or circulating any material that is of a racist, misogynistic or otherwise hateful nature. Verco explicitly states that it has the right to monitor any use and logs on use are kept. Attempts to access any prohibited sites are automatically flagged to the IT department, who after three times pass on the alert to the relevant department / line manager. It is the department / line manager's obligation to raise the issue with the relevant employee and to issue a warning if necessary. There have been no warnings issued in the last two years, despite some employees reporting that colleagues had used their own laptops to access inappropriate material during office hours. Line managers reported that even when they did get an alert, they did not always feel comfortable raising the issue with an employee, and felt that there was no sufficient guidance to explain to them how to breach the topic and issue warnings.	
Recommendations:	
Verco should consider offering training sessions to line manager on how to address inappropriate user behaviour, and stress the importance of following the appropriate use policy. In addition, Verco may wish to consider a blanket ban on the use of personal laptops and other hand held devices during office hours, and re-circulate its communication about what may and what may not be accessed or circulated by employees during office hours or using office equipment.	

OP14: The organisation has a clear process to review any personal data it holds, where it has come from and with whom it is shared.	Grade: Merit
A process is in place which automatically flags up personal data that has been held for a period of 18 months, in 18 months' intervals, prompting the marketing and sales department to verify if the data is still correct, to verify its origin and whether it has been shared and with whom. An email is sent to the relevant data subject to confirm the personal data, and to inform him or her of what data is being held.	
Assessment:	
The review of personal data is clear and regular. It is unclear how much time should pass before a reminder is sent to the data subjects if they do not respond to emails, but a clear rule exists that if there is no reply after	

4 months, any non-essential data (i.e. necessary to the performance of the contract or customer relationship) is erased.
Recommendations:
A clear guideline how often and in what intervals the data subject should be reminded to respond after the initial email should be implemented and shared among all relevant employees.

OP15: The organisation has a system in place to consider the most appropriate way of sharing data, including where appropriate by way of pseudonymisation.	Grade: Merit
Verco has clear rules and processes in place in relation to sharing data, focussing mainly on ensuring that consent or necessity exists for the sharing of data, and that appropriate safeguards are in place with the recipients of data.	
Assessment:	
Before any data is shared with outside recipients, the sender must confirm that he has considered the appropriateness of sharing data and that safeguards are in place to guarantee secure handling of the data – this includes verifying if the data requires sharing, if the data protection policies and processes of the recipient are acceptable, and if it is necessary to reveal personal data or if some data can be anonymised.	

OP16: Data is kept up to date as necessary and a system is in place to identify inaccuracies and, where relevant, to correct them.	Grade: Merit
As mentioned in OP14, data held automatically gets flagged every 18 months for a verification exercise.	
Assessment:	
In addition to the email sent to the data subject (see OP14), Verco employees (usually in the Sales and Marketing department), are asked to check if there is any information that suggests the personal data must be updated or changed, e.g. if they have received letters marked “non-deliverable’, or if they have received any correspondence from the relevant data subject.	

OP17: There are rules governing the temporary or permanent removal of data, whether hard-copy or electronic, from the organisation's secure sites.	Grade: Merit
A separate handbook exists for the removal of any data, whether temporary or permanent, or hard-copy or electronic. The IT department is the only department which has employees authorised and able to remove any electronic data from Verco's secure sites.	
Assessment:	
Any requests to remove any data from Verco's secure sites must go through the IT department, which is specifically trained to consider the rules relating to the temporary or permanent removal of data. When in doubt, it is mandatory to reach out to Verco's legal department and/or the data protection team. For hard copies, the employment handbook, the data protection policy, and the separate handbook for the removal of data, all specify that and permanent removal must be done securely, and any destruction must be done using the shredding machines available in each store and in the head office. These machines all carry warning signs to consider whether the removal is necessary and has been considered fully, and provides the contact details of the data protection team and the legal department in case of doubt or questions.	

OP18: The organisation recognises data subjects' right to erasure and has a system in place which addresses such requests.	Grade: Observation
The publicly available privacy notice mentions a data subject's right to erasure, and specifies that a system exists to address such requests. The internal data protection policy refers to a documents entitled "Dealing with Data Subjects' Requests" which is available on Verco's intranet and has last been updated in July 2016.	
Assessment:	
The document "Dealing with Data Subjects' Requests" is a comprehensive guidance document to addressing the various types of potential data subject requests, from access requests to erasure requests. It sets out exactly how these requests should be dealt with and who is responsible for them, in a clear and easily accessible flowchart. Any request is supposed to be logged and the data protection team is responsible for keeping the log book up to date and following up on any outstanding entries. 2 of the interviewed customers reported that they had made requests (access requests in both instances) but had not heard back anything and were therefore understandably not satisfied with the way their requests were handled. Both complaints were in fact recorded in the requests log book, but had not been followed up on. Some of the receptionists and front-line staff interviewed were not confident about how to deal with any data subject request, and were not aware that a specific document on how to deal with any requests existed, though they did suggest they would be likely to find it once they started looking for it on the intranet website. Indeed, the document is prominently displayed on the homepage of the "Data Protection and Information Sharing" tab on Verco's intranet site.	

Recommendations:
Training for receptionists and anyone who is customer-facing should include a dedicated section on how to deal with data subject requests. It may also be helpful to send out regular reminder emails (once a month) to highlight the relevant policies and where to access them. The data protection team should ensure that the log book is inspected carefully on a regular basis (at least once to twice a week) and that any outstanding entries are dealt with as soon as reasonably practicable.

OP19: Data is disclosed to third parties only by those with authority to do so.	Grade: Observation
A list of those with authority to disclose data to third parties is kept by the data protection team. For each employee, an assessment is made whether authority is needed, depending on its role and job category. Some employees, such as store staff, automatically get authority by virtue of their role and interaction with customers.	
Assessment:	
Only those authorised to do so disclose data to third parties, but the list of people with authority to do so is large and encompasses a majority of staff. Of the interviewed employees, 86% were authorised to disclose data according to their employee profile. Some of the staff, such as store staff, are automatically allowed to disclose data without any assessment of whether they need to be able to do so. Given the sharing of data of stores with the head office and other points of contact (banks and other finance institutions, credit check providers, etc.) being necessary to provide customer services, this makes sense – however, staff includes cleaners on some sites: in Nottingham and Birmingham Verco employs his own cleaners who have the same rights and disclosure status as other Verco employees on those sites; in London and Bristol cleaning is contracted out (and no such privileges are granted). This is likely an oversight (and the cleaners interviewed did not have any access to personal data), but there is no reason why all staff in stores should automatically get disclosure rights.	
Recommendations:	
Verco should not use categories to allow general authority to employees, but should allocated authority on strict basis of necessity and consider the duties and job description of each employee before giving the employee data sharing authority.	

OP20: Data is held for a defined period of time or until the need for it has passed and then the data is securely suppressed or deleted.	Grade: Merit
As mentioned in OP14, data is regularly reviewed every 18 months. If the review reveals that the data is no longer needed, or consent or necessity to use the data no longer exists, then the data will be securely surpassed or deleted.	
Assessment:	
Each contract sets out clearly the timeframe for which data is held, and that the data will be deleted if it is no longer needed or if consent to use it is no longer forthcoming (subject to any legal requirements). Before any data is suppressed or deleted, it is possible to reach out to the data protection team and the legal team to verify if the deletion is appropriate.	

OP21: Processes exist to destroy data or to render it irrecoverable. Confidential waste is properly handled.	Grade: Commendation
The processes in place to destroy data or to render it irrecoverable are set out in the internal data protection policy. Any data which is stored off-site with CloudStorage (the vast majority of data) and needs to be destroyed, is destroyed by CloudStorage itself, after a confirmation process. A contractor comes to the site three times a week to collect any shredded material and other confidential waste.	
Assessment:	
The processes to destroy data are very clear and involve steps taken by the data protection team, the legal team and CloudStorage. Any data which is to be destroyed permanently must have obtained (electronic agreement) by the data protection team and the legal team (through a simple online ticking exercise). Before CloudStorage proceeds to destroy data, it sends across a summary document of the data to be destroyed and awaits Verco's final confirmation. An outside contractor of very good reputation, ConfiShredder Ltd, picks up confidential waste from all of Verco's offices and stores across the UK on a thrice-weekly basis, and transports any waste in locked steel bins to the local incinerator plant. A staff member of ConfiShredder Ltd. ensures that all material is burnt before leaving the site, and ConfiShredder invites its customers to join the process and inspect at any time – which Verco has done on two occasions, in June 2013 and July 2015.	

OP22: Data is securely erased from equipment prior to the equipment's disposal.	Grade: Merit
The internal data protection policy covers the secure deletion of data on any equipment that is about to be disposed of. All of Verco's electronic equipment contains a remote-erasure software.	
Assessment:	
All electronic equipment must be returned to the IT department if it is faulty or if it needs to be disposed of. The IT department has clear instructions and facilities to back up on an external server any data contained on the equipment, and to securely erase the data on the equipment itself. The methods used are state-of-the-art and ensure that there is no recovery process that can be undertaken to recover, at a later point, any of the data once present on the relevant equipment. In addition, it is possible to remote erase any data on any equipment, in case it gets lost or stolen.	

OP23: The organisation has additional safeguards in place for the processing of sensitive personal data.	Grade: Merit
Both the publicly available privacy notice and the internal data protection policy stipulate the additional safeguards in place for the processing of sensitive personal data. Before such data is processed, approval must be obtained from a member of the data protection team. Any collection of such data on paper or electronically is prefaced by a separate text asking the collector whether the information is actually necessary, and to limit such collection to the minimal possible.	
Assessment:	
Verco has additional safeguards in place for the processing of sensitive personal data. The internal policy has a dedicated section on sensitive data which sets out clearly what the grounds are to process sensitive personal data, and the ground of consent has been updated to reflect the new GDPR requirements. The policy also gives a list of what is considered sensitive personal data, namely: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • data concerning health or sex life and sexual orientation. This does not reflect the GDPR, which also explicitly encompasses genetic data and biometric data where processed to uniquely identify a person. Given that fingerprints and biometric data are routinely used now as part of any telecommunications, this is data that should be specifically mentioned. While Verco does already	

treat genetic and biometric data as sensitive, it may be advisable to include it specifically in the list set out in its policy.
Recommendations:
Verco should update its policies to clearly include genetic and biometric data as sensitive data.

6. Managing employees who handle data

ME1: Employees receive periodic training on data protection and, where relevant, on how to handle data protection queries.	Grade: Observation
Each new employee is required, upon joining Verco, to undertake the firm-wide e-learning on data protection which takes approximately 45 minutes. This training has to be retaken annually. A test at the end of the e-learning checks knowledge, and employees have to obtain 90% before they are considered to have completed the training. Dedicated training is provided, usually by external providers, to the members of the data protection team.	
Assessment:	
The training on offer is slightly lacking in respect of customer-facing staff / receptionists and could be more frequent, as set out in OP18. There is no tailored training for staff apart from the additional, external training offered to the members of the data protection team. This means that all employees receive the same training on data protection, no matter how relevant the issues are to any particular employee.	
Recommendations:	
Verco should tailor specific training according to an employee's needs. Basic overall training is a good idea, but additional training should be considered for those who are likely to have to deal with requests, process large amounts of personal data (HR staff members, customer-facing employees) etc.	

ME2: The person designated as being responsible for data protection within the organisation receives specific training and is aware of a data protection officer's tasks and responsibilities.	Grade: Merit
Miguel Samarrco is Verco's data protection officer. He has a dedicated training plan which includes training sessions on management skills and data protection related topics.	
Assessment:	
Miguel Samarrco receives specific training and is aware of his tasks and responsibilities as data protection officer. The data protection officer at Verco must undertake at least 3 training days and is entitled to up to 10 training days a year in order to further his job knowledge, with a possibility to extend if the additional training is approved by his supervisor and justified by its content and Samarrco's need. Additional training is also offered to the rest of the data protection team. Other staff members are entitled to join in but must do so out of their own initiative and are not guaranteed to be able to use a work day for attending – this must be confirmed on a case-by-case basis by their direct supervisor.	

ME3: There are regular communications campaigns to raise employees' awareness of data protection.	Grade: Observation
The last general communication campaign on data protection was undertaken in January 2015, by email. Before that, a campaign to raise awareness was undertaken in October 2012, by distributing "data protection info kits" to all employees. Specific emails on a variety of topics (such as phishing or other email scams, clear-desk policy, choosing adequate passwords and other privacy related matters) are sent on an ad-hoc basis.	
Assessment:	
While communication emails are sent out fairly regularly, there is no formal system and no clear idea of what topics will be covered. The communications campaigns lack structure and are organised on an ad-hoc basis as the data protection team and colleagues from legal or senior management see fit.	
Recommendations:	
Verco should consider spending some time setting up a clear communications plan with respect to data protection issues, responding not only to specific topics or matters of urgency, but also ensuring that data protection reminders are sent in regular intervals, with links and information for employees to refresh their knowledge and raise overall awareness.	

ME4: Data protection policies and procedures are readily accessible for employees' reference.	Grade: Merit
Any policies and procedures, including those relating to data protection, are on Verco's intranet.	
Assessment:	
The data protection policies and procedures are readily accessible for the employees' reference, across all of Verco's operations. Each employee has a personalised log-in for Verco's staff intranet, which contains a dedicated section on data protection policies and procedures.	

ME5: Employees are subject to written contractual confidentiality obligations.	Grade: Merit
The employment contract, as well as any agent or freelancer contracts, contain confidentiality obligations.	

Assessment:
The written contractual confidentiality clauses are binding on each employee and third party hired by Verco, as well as on Verco itself. They are comprehensive and cover all the relevant areas.

ME6: Disciplinary processes are used to support observance of data protection policies.	Grade: Minor non-compliance
According to the Code of Conduct, disciplinary processes are mandatory should the data protection policy not be observed. No records exist of a formal disciplinary process having started because of an infringement of the data protection policy.	
Assessment:	
All infringement of Verco's key policies, of which the data protection policy is one, are subject to disciplinary processes. It is clearly stated in the Code of Conduct that disciplinary processes are used to support observance of those policies. A strong majority of employees were certain that if someone did infringe the data protection policy, a formal disciplinary process would be set in motion. However, there is no record of a formal disciplinary process ever have been triggered by a non-observance of the data protection policy. Given that several data protection policy infringements have been noted in the past, were reported by the interviewees and have been noted by the assessors during the assessment (such as storage spaces not being locked by key, desks not being kept clear, inappropriate use of private devices), there seems to be a disconnect between the actions of employees and the enforcement of data protection rules. There is also no clear picture of what that disciplinary process would in fact encompass – the Code of Conduct contains only a general statement to the effect that "disciplinary processes will be set in motion in relation to any infringement of any policies, including the sending of warning letters and, as a last resort, ultimate dismissal from the employee's post."	
Recommendations:	
Verco should set out in more detail what its disciplinary process entails and what the different steps are from the first formal warning letter to the ultimate sanction of dismissal. This should be contained in an updated Code of Conduct. Verco should further ensure that the formal disciplinary process is actually used in respect of data protection infringements to signal that it is serious about the respect of its data protection policies. A formal first warning letter to employees in breach of a data protection rule, setting out what the infringement is, how to avoid such infringement and offering to discuss and/or provide further clarification in person would be a good first step. In addition, Verco may wish to consider including a sample (fictitious or anonymised) case study in its Code of Conduct or its data protection policy on how the disciplinary process would be used in respect of infringements of the organisation's data protection rules.	

7. Managing routine access by third parties

TP1: The organisation communicates its data protection policies and standards clearly to service providers and business partners.	Grade: Observation
Verco usually sends its data protection policy and standards to service providers and business partners as part of the contracting process (and before any final contract is entered into). All contractual documents include a part for a third party to acknowledge receipt and understanding of the data protection standards.	
Assessment:	
Before any contractual relationship with service providers and business partners is set up, Verco asks that the third party has acknowledged and understood Verco's policies and standards. In some cases, the data protection policy and standards are specifically emailed to the third party together with any contractual documentation and the Code of Conduct. In other cases, the third party is asked to verify the policy and standard itself by accessing them online. About 60% of the third parties interviewed which did not receive a specific email with the policies acknowledged that they had not, in fact, verified the data protection policy in advance, even though they were asked by Verco whether they had and were required to make a statement to that effect.	
Recommendations:	
Verco should ensure that the data protection policy and related standards are communicated by email in advance in each case, and not rely on the third party to obtain the documents itself instead.	

TP2: The organisation ensures that service providers' or business partners' data protection practices are adequate prior to instructing them to collect, handle or destroy data on its behalf.	Grade: Minor non-compliance
Verco obtains a contractual statement that its service providers or business partners which collect, handle or destroy data on its behalf meet Verco's data protection policies and standards, and asks them to familiarise themselves with those standards, acknowledging that they have read and understood them (see TP1) as well as having adequate practices themselves.	
Assessment:	
Other than the contractual statement, and occasionally verifying whether the service provider or business partner has a data protection policy at all, Verco does not check the actual content of any such policy. Nothing appears to be done beyond ensuring that a statement confirming adequate practices is obtained; there is no actual verification or subsequent diligence on the other party.	
Recommendations:	

Verco is aware of the importance of service providers and business partners having adequate data protection practices if they are to collect, handle or destroy data on Verco's behalf. This is demonstrated by its insistence on those other parties to provide contractually enforceable guarantees to that effect. However, Verco should make sure that it verifies at least some of its service providers' or business partners' data protection practices to show its own commitment and safeguard against infringements in its supply chain.

TP3: The organisation imposes adequate contractual obligations on service providers or business partners relating to data protection.	Grade: Merit
Contracts with third parties all include obligations relating to data protection.	
Assessment:	
Verco ensures that across its contracts with its service providers or business partners, data protection obligations are included and clearly set out. They form part of Verco's boilerplates in its suite of contracts, and were present in every contract that was reviewed for the assessment, as well as every template contract.	

TP4: The organisation actively manages its service providers or business partners to ensure data is properly protected.	Grade: Observation
Service providers or business partners must sign up to data protection obligations when entering into a contract with Verco. When data is transferred between the service provider or business partner and Verco, Verco sends its data protection policy and a reminder of the contractual obligations as a matter of routine.	
Assessment:	
Verco is strong in making sure that the contractual obligations in relation to protecting data are clearly stipulated and reminds its service providers or business partners of its policies and of the obligations in a regular fashion. However, the reminders are the full extent of Verco's active management, and there is no further follow-up, feedback or verification of how data is handled by the third parties.	
Recommendations:	
Verco should consider enacting a more formal process in relation to the active management of its service providers' or business partners' handling of data and the protection thereof. It could consider asking for periodic feedback and actively engaging with its business partners or service providers in offering data protection training and checking their commitment to data protection.	

TP5: The organisation conducts spot checks on service providers or business partners to ensure compliance with its standards.	Grade: Minor non-compliance
The contracts in place with service providers or business partners contain a right for Verco to audit its contractual partners to ensure compliance with its standards, including the carrying out of spot checks.	
Assessment:	
While the contractual framework is in place, Verco does not conduct spot checks to ensure compliance and the system in place does not appear to be used (see TP2).	
Recommendations:	
Verco should include spot checks, starting with key service providers or business partners that handle large volumes of data on behalf of Verco.	

TP6: The organisation imposes sanctions where service providers or business partners fail to meet its required standards for data protection.	Grade: Observation
Across its contracts, Verco has specific termination clauses as well as damages and mitigation clauses which apply to service providers or business partners where they fail to meet Verco's required standards for data protection.	
Assessment:	
While Verco has the right to impose sanctions where its required standards for data protection are not met, it has never had to impose any. Contractually, Verco has robust sanction rights, and there are clear consequences for data protection failures. However, the lack of post-contractual verification on Verco's side renders the sanctions process theoretical, and it is difficult to assess if any sanctions should have been employed but weren't.	
Recommendations:	
While there is no suggestion that service providers or business partners have in fact failed to meet Verco's required standards for data protection, Verco should strongly consider (as set out in TP2 and TP4) a verification process and spot checks to ensure compliance, and enable it to use its contractual rights to sanction where necessary.	

8. Managing Requests

RQ1: Protocols are in place governing the disclosure of data (credentials, criteria, legal advice, requirements placed on recipient etc.).	Grade: Merit
Flowcharts and guidance documents are available on Verco's intranet in respect of the applicable protocols for disclosing data.	
Assessment:	
The available guidance sets out the protocols in place, explaining what steps to take and what the prerequisites are before any data may be disclosed. Each guidance contains, at the bottom of several pages, prompts to reach out to the data protection team (with an email and a number to call) should there be any questions or uncertainties.	

RQ2: The organisation responds to public authorities' requests for data constructively and responsibly.	Grade: Not applicable
There has never been a request by any public authority for data.	
Assessment:	
Not applicable.	

RQ3: There are clear processes in place to respond to data subjects' requests, including: • for access; • to have inaccuracies corrected; • to prevent direct marketing; • to prevent automated decision-making and profiling; and • for data portability.	Grade: Merit
The intranet contains guidance and flowcharts to address data subjects' requests, including the five listed above.	

Assessment:
As set out in RQ1, each of the data subjects' requests is addressed in internal guidance and flowchart, easily accessible on Verco's intranet; if a need for further clarification exists, then contact points are unequivocally identified and people are encouraged to reach out to the relevant data protection representatives.

RQ4: Systems are in place which clearly establish the decision-making process in response to any type of request, and such systems are understood within the organisation.	Grade: Merit
As part of the guidance, which includes the flowcharts (see RQ1 and RQ3), the decision-making process is set out.	
Assessment:	
The flowcharts make the decision-making process easy to understand and to follow. Each level of management can refer to its position in the flowchart and find out who to speak to, who to escalate an issue to, and who to distribute or inform of any particular issues.	

9. Breaches

BR1: IT systems and data storage facilities are regularly checked for any data breach.	Grade: Observation
The IT department checks for any internal server breaches every last Friday of the month. According to the general T&Cs of CloudStorage, there is ongoing monitoring of all of its stored data, and a dedicated verification of any breaches once a week.	
Assessment:	
Both internal storage facilities and external facilities undergo regular checks for data breaches. However, Verco may consider to change its times to avoid repetitive behaviour, and have the monthly checks on different days of the month. In addition, at the moment no detailed records are kept of each check – according to Verco's internal policy, there should be a report after each check, but Verco's IT department was unable to produce a completed report for two of the last six months. No reports have ever been requested from CloudStorage on their data breach checks, even though this forms part of Verco's rights. CloudStorage has comprehensive reports dating back 7 years for each of its checks, and is willing to send executive summaries and/or complete reports to its clients (subject to the applicable confidentiality provisions) in pdf form.	
Recommendations:	
Verco may wish to consider changing the times when it checks for data breaches to avoid any repetitive or typical behaviour. It should further ensure that the reports on each check are diligently filled in and properly filed. Finally, it may wish to consider asking for and reading the reports on the checks conducted by CloudStorage to keep an eye on its external IT systems and data storage facilities.	

BR2: Staff are aware of whom they should speak to if they suspect a data breach.	Grade: Commendation
If a data breach is suspected, the Code of Conduct and the data protection policy set out that staff should speak to their supervisor and inform Verco's data protection team.	
Assessment:	
Whom to speak to in case of a suspected data breach is clearly set out, and all employees interviewed bar one have a clear and accurate idea of whom to address should they suspect any data breach. This information is also contained in the online induction training all staff have to undergo upon joining. Moreover, it forms part	

of the "Who to speak to" flowchart available on the intranet which sets out in an easy to comprehend manner who should be addressed in a variety of situations.

BR3: There is a confidential means of reporting data protection concerns.	Grade: Observation
The whistleblowing policy mentions that it can also be used to report any data protection concerns.	
Assessment:	
None of the interviewees were aware of the confidential means of reporting data protection concerns, but almost uniformly indicated they would know who to speak to and would not be concerned about confidentiality. When asked if they would consider using the whistleblowing hotline to report data protection concerns, the interviewees in almost their entirety had not considered this, and were under the impression that such hotlines are only for issues such as bullying and harassment.	
Recommendations:	
Verco should consider revising its data protection policy to include an explicit reference to the whistleblowing hotline as being a means of reporting any data protection concerns confidentially. It would also be helpful to add that information to the induction training and make it as well known as the identity of those the staff should speak to if they have any queries.	

BR4: The organisation has a protocol governing data breaches, that includes information on how to respond and how to inform the affected data subjects as well as notify the relevant authority of the breach in a timely fashion and without undue delay.	Grade: Merit
A dedicated "Data Breaches" document provides guidance as to what to do in case of data breaches.	
Assessment:	
The available guidance (at the top of the "Data Protection" website on the intranet) sets out clearly, in form of a checklist, what the protocol governing data breaches is. It provides a helpful flowchart to understand each required step, and sets out who should be notified internally and, if necessary, externally, and what the timeline is. A very good 24 hours from the discovery of a breach are set as the usual target timeline to make all of the necessary internal and external notifications.	

BR5: The organisation investigates the causes of data breaches and takes remedial action.	Grade: Not applicable
No data breach has ever been identified.	

BR6: The organisation works proactively with authorities investigating potential breaches.	Grade: Not applicable
No breach has been reported or detected. As of mid-August 2016, there had never been an occasion to work with authorities investigating potential breaches.	

10. Monitoring and review

MR1: The documentation requirements for the various sets of data are regularly reviewed, and a clear process is in place to identify the organisation's record keeping obligations.	Grade: Merit
Each set of data held is recorded in a log, which also includes information on the type of data and the record-keeping obligations in relation to that type. The log is updated by the different departments, and a guidance document available on the intranet enables employees to identify what the documentation requirements and Verco's record-keeping obligations are.	
Assessment:	
The log containing the different data sets is clear and updated regularly. It is in electronic format and has an easy to use search function. For each new entry, it prompts the person entering the data to consider the documentation requirements and will not allow an entry to be saved unless the requirements and record-keeping obligations are acknowledged by the employee. There is a clear process in place which allocates the review of the documentation requirements for the various sets of data to the data protection team, which is also tasked with ensuring that Verco's record-keeping obligations are kept.	

MR2: There is a regular review by senior management of the effectiveness of existing data protection measures.	Grade: Observation
The data protection team meets at least once a month, as does the legal team.	
Assessment:	
The data protection team as well as Verco's legal department regularly reviews existing data protection measures and has regular meetings to discuss any issues and changes to the legal obligations. There is no regular consideration by senior management as such of the effectiveness of existing data protection measures; instead, changes and issues are raised on an ad-hoc basis by the data protection team and/or the legal team.	
Recommendations:	
Verco may wish to consider including the effectiveness of existing data protection measures as a standing order agenda item at board meetings.	

MR3: There are periodic audits of the management of data protection.	Grade: Merit

Verco operates a system of internal auditing on an 18-month basis for its different departments, meaning that each 18 months, each department is subject to an internal audit process.
Assessment:
The internal audit system specifically includes data protection management and detailed records are kept of each audit, including a list of shortcomings and weaknesses and a proposed action plan, with progress reviews scheduled in for 3 months and 8 months after the conclusion of each audit.

MR4: The organisation conducts periodic unannounced simulations of breaches and attacks which could potentially compromise data protection and privacy.	Grade: Minor non-compliance
As simulated attack, by way of phishing emails sent to employees by Verco's IT department, was conducted in June 2015, with the results and recommendation being distributed to all employees at the end of July 2015. The data protection team envisages at least one such type of simulation each year going forward (the next one is scheduled for October 2016).	
Assessment:	
Verco is aware of the threat emanating from cyberspace, and has realised that simulations and fake attacks are very useful in identifying weaknesses and technological as well as operational shortcomings. Its commitment to conduct unannounced simulations yearly is proof of that. Last year's simulation was followed up by a clear summary and practicable recommendations given to all employees. However, the attacks are, at the moment, still ad-hoc and do not span a wide enough range of threats – it is insufficient to focus just on one threat as part of each simulation. Nor do the current fake attacks involve any third parties or expert "friendly" attackers, thereby potentially missing out on professional, state-of-the-art simulations.	
Recommendations:	
Verco should consider reaching out to external service providers to arrange for simulations of breaches and attacks. This should include a longer-lasting arrangement (at least 6 months), in which Verco is being tested in different ways (hacking attacks, phishing emails, spoofing, botnets, pharming and other types of common cyber security threats), and an ongoing agreement to carry out regular simulations and attacks to ensure that Verco is continuously up to speed with its data protection.	

MR5: There is a periodic report to the board on data protection, along with information and indicators on data breaches.	Grade: Observation

As explained in MG6, Miguel Samarrco, the current data protection officer, has a direct reporting line to the board. However, he is not a regular participant in any board meetings. Information and indicators on data breaches would be transmitted on an ad hoc basis.
Assessment:
Please refer to the assessment box in MG6 above.
Recommendations:
As mentioned in MG6, data protection should become a standing order agenda item at each board meeting. In addition, Verco may wish to consider obliging the data protection team to provide a more detailed report, perhaps once every six months, on any issues and information in relation to data protection and data breaches.

Appendix 2 Document Log

[*Intentionally left blank*]

Appendix 3 Meeting Log

[*Intentionally left blank*]