CORSERV

CORSERV LIMITED
Data Protection Policy

Date 1/11/2018 v1.0
Company Secretariat Office

A CORNWALL COUNCIL COMPANY

As the parent Company, Corserv aims to unify key policies across its Group of Companies.

This document forms part of a suite of policies that apply to each Company within the Corserv Group. They supersede any previous Company-specific documentation relating to the same subject matter named on the front of this Policy.

1. INTERPRETATION

1.1 KEY TERMS

Company: Corserv Limited and its subsidiary companies including: Cormac Solutions Limited, Cormac Contracting Limited, Cornwall Housing Limited, Cornwall Development Company Ltd and Cornwall Airport Newquay. Also referred to as "the Company", "we", "our" or "us" in this policy.

Data Controller: the person or organisation that determines when, why and how to process personal data. We are the data controller of all personal data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold personal data.

Data Privacy Impact Assessment (DPIA): an assessment to identify and reduce data protection risks of a data processing activity or project.

Data Protection Act 2018: The legislation which ratifies the GDPR in English law.

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes the special categories of personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. The

GDPR and Data Protection Act 2018 apply to any information held about a living, identifiable individual.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Privacy Notices: notices setting out information that may be provided to data subjects when we collect information about them.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Special Categories of Personal Data: personal data concerning racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. INTRODUCTION

2.1 This policy sets out how we handle the personal data of our directors, officers, employees, customers, suppliers, consultants, contractors, workers, volunteers and other third parties in compliance with the GDPR and Data Protection Act 2018.

2.2 This policy applies to all personal data we process regardless of whether it is in electronic form or hard copy or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, volunteers, website users or any other data subject.

2.3 This policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the Data Protection Officer.

2.4 This policy does not form part of any employee's contract of employment. We shall keep this policy under regular review and may amend it from time to time.

2.5 This policy has been implemented following consultation with the trade unions recognised by the Company.

2.6 This policy shall supersede and replace any other individual Corserv Group Company policy relating to this subject matter.

3. SCOPE

3.1 Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. We are exposed to potential fines of up to the higher of EUR20 million or 4% of total annual turnover for failure to comply with the provisions of the GDPR. Therefore, it is important that everyone complies with this

policy.

3.2 This policy applies to all employees, workers, contractors, volunteers, agency workers, consultants, directors and officers and to any other third party who processes personal data on our behalf. You must ensure that you read, understand and comply with this policy when processing personal data as part of your work duties. Your compliance with this policy is mandatory. Any breach may result in disciplinary action.

3.3 The Corserv Board of Directors have overall responsibility for the effective operation of this policy.

3.4 The Group Data Protection Officer (GDPO) is responsible for overseeing this policy. This post is held by Richard Zmuda, Group Company Secretary (contact details are set out in Paragraph 22).

3.5 Please contact the GDPO with any questions about the operation of this policy or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the GDPO in the following circumstances:

3.5.1 if you are unsure whether you can lawfully process personal data (see Paragraph 5);
3.5.2 if you need to obtain consent to process personal data (see Paragraph 6);
3.5.3 if you need to draft privacy notices (see Paragraph 7);
3.5.4 if you are unsure about how long personal data may be retained for (see Paragraph 11);
3.5.5 if you are unsure about what security or other measures you need to implement to protect personal data (see Paragraph 12);
3.5.6 if there has been a personal data breach (Paragraph 13);
3.5.7 if you become aware that personal data is to be transferred outside the EEA (see Paragraph 14);
3.5.8 if you need any assistance dealing with any rights invoked by a data subject (see Paragraph 15);
3.5.9 if you receive a data subject access request (see Paragraph 16);
3.5.10 if you feel that a Data Privacy Impact Assessment (DPIA) may be required (see Paragraph 19) or plan to use personal data for purposes other than what it was collected for;
3.5.11 if you plan to undertake any activities involving automated processing including profiling or automated decision-making;
3.5.12 if you need help complying with the GDPR and Data Protection Act 2018 when carrying out direct marketing activities (see Paragraph 20); or
3.5.13 if you need help with any contracts or other areas in relation to sharing personal data with third parties (including our vendors) (see Paragraph 21).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 The GDPR requires personal data to be:

4.1.1 processed lawfully, fairly and in a transparent manner;
4.1.2 collected only for specified, explicit and legitimate purposes;
4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for

which it is processed;

4.1.4 accurate and where necessary kept up to date;

4.1.5 not kept for longer than is necessary for the purposes for which it is processed;

4.1.6 kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage;

4.1.7 not transferred to another country without appropriate safeguards being in place; and

4.1.8 made available to data subjects and to allow data subjects to exercise certain rights in relation to their personal data.

4.2 Accountability is a key principle of the GDPR. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above. Everyone is responsible for complying with the data protection principles set out in this policy.

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 Personal data must be processed lawfully, fairly and in a transparent manner. You may only collect, process and share personal data for lawful and specified purposes.

5.2 The GDPR allows processing for specific purposes, which include:

5.2.1 the data subject has given his or her consent;

5.2.2 the processing is necessary for the performance of a contract with the data subject;

5.2.3 to meet our legal compliance obligations;

5.2.4 to protect the data subject's vital interests; or

5.2.5 to pursue our legitimate interests.

5.3 Prior to processing any personal data you must identify the legal ground that is being relied on. If you are unsure what the correct legal ground is then please contact the DPO.

6. CONSENT

6.1 We may process personal data if we obtain consent to do so.

6.2 A data subject consents to the processing of their personal data if they indicate agreement clearly, either by a statement or positive action, to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient methods of demonstrating consent. If consent is given in a document which deals with other matters, then the consent itself must be kept separate from those other matters.

6.3 Data subjects must easily be able to withdraw their consent at any time. Consent must be re-obtained if you intend to process personal data for a different purpose which was not disclosed when consent was first obtained.

6.4 You must keep records of any consent obtained so that we can demonstrate our compliance with the GDPR.

7. TRANSPARENCY AND PRIVACY NOTICES

7.1 The GDPR requires us to provide specific information to data subjects. The information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them.

7.2 Whenever we collect personal data directly from data subjects, including data collected for human resources or employment purposes, we must tell them the identity of the data controller and GDPO, and how and why we will use, process, disclose, protect and retain their personal data.

7.3 When personal data is collected indirectly (for example, from a third party or publicly available source) we must provide the data subject with a privacy notice as soon as possible after collecting or receiving the data. We must also check that the personal data was collected by the third party in accordance with the GDPR.

7.4 If you are collecting personal data, directly or indirectly, then you must provide a privacy notice to the data subjects. For assistance with this requirement please contact the GDPO.

8. PURPOSE LIMITATION

8.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner which is incompatible with those purposes. You cannot process personal data for any new or different purposes; you must only process it in accordance with the purpose it was originally collected for.

9. DATA MINIMISATION

9.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

9.2 You may only process personal data when the performance of your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

9.3 When personal data is no longer needed for the specified purposes it was collected for, then it must be deleted in accordance with our data retention guidelines.

10. ACCURACY

10.1 You must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

11. STORING PERSONAL DATA

11.1 You must not keep personal data for longer than needed in accordance with the purpose for which it was originally collected (including for the purpose of satisfying any legal, accounting or reporting requirements).

11.2 We will maintain retention procedures to ensure personal data is deleted after a reasonable time, unless a law requires that data to be kept for a minimum time. A copy of the retention guidelines can be obtained from one of the contacts listed in Paragraph 22.

11.3 You must take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with our record retention guidelines. This includes requiring third parties to delete that data where applicable.

11.4 You must ensure data subjects are informed of the period for which data is stored and how that period is determined in any privacy notice.

12. SECURITY AND CONFIDENTIALITY

12.1 Personal data must be kept secure by appropriate technical and organisational measures to prevent unauthorised or unlawful processing, and against accidental loss, destruction or damage.

12.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and other identified risks. You are responsible for protecting any personal data that you process as part of your role from loss and unauthorised access, use or disclosure. You must follow all procedures we put in place to maintain the security of personal data.

13. REPORTING A PERSONAL DATA BREACH

13.1 The GDPR requires us to notify any personal data breach to the regulator (the Information Commissioner) and in certain circumstances, the data subject. Certain breaches must be notified to the Information Commissioner within 72 hours of discovery.

13.2 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for personal data breaches (see Paragraph 22) or the GDPO. Do not notify the data subject yourself.

13.3 It is everyone's responsibility to ensure that all personal data breaches are reported in accordance with this policy.

14. TRANSFERRING PERSONAL DATA OUTSIDE OF THE EEA (EUROPEAN ECONOMIC AREA)

14.1 The GDPR restricts data transfers to countries outside the EEA unless adequate measures of protection are in place.

14.2 If you believe that you, one of our suppliers or another third party engaged by us, needs to transfer our personal data outside of the EEA, then you must notify the GDPO.

15. DATA SUBJECT'S RIGHTS AND REQUESTS

15.1 Data subjects have rights when it comes to how we handle their personal data. These include rights to:

15.1.1 withdraw consent to processing at any time;
15.1.2 request access to their personal data that we hold;
15.1.3 prevent our use of their personal data for direct marketing purposes;
15.1.4 ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data;
15.1.5 request a copy of an agreement under which personal data is transferred outside of the EEA; and
15.1.6 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms.

15.2 We must verify the identity of an individual requesting data under any of the rights listed above.

15.3 You must immediately forward any data subject request you receive to the GDPO.

16. SUBJECT ACCESS REQUESTS

16.1 Data subjects have the right to receive a copy of the personal data that we hold about them. Upon receipt of a valid request and verification of the relevant identification documents, we will provide a statement confirming what personal data we hold, process, the reasons for the processing it and how long we will store it for.

16.2 All requests should be submitted in writing to the GDPO. We will respond promptly and in any one event within one month of receiving the request. Before responding we will check the identity of the person making the request pursuant to paragraph 15.2.

16.3 In some cases, for example where we process large amounts of an individual's data, we may respond in a period longer than one month. We will write to the individual within one month of receiving the original request to advise them if this is the case.

16.4 If a subject access request is manifestly unfounded or excessive, then we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a reasonable fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it is a repeat of a request to which we have already responded.

17. FREEDOM OF INFORMATION ACT 2004

17.1 The Freedom of Information Act 2004 (FOIA) allows members of the public to request information from public authorities (FOIA Request). As we are wholly owned by Cornwall Council we may be required to provide certain information.

17.2 If you receive a FOIA Request then you must refer it to either the GDPO or one of the contacts listed in paragraph 22 without delay.

18. TRAINING

18.1 You must undergo all mandatory data privacy related training that you are directed to complete regarding compliance with data privacy laws.

19. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

19.1 The purpose of a DPIA is to systematically analyse, identify and minimise any data protection risks in a project or plan. We must conduct DPIAs in respect of any high-risk processing. This could be, for example, where you are required to process special category personal data on a large scale.

19.2 We must also conduct a DPIA when implementing major new business systems or business change programs involving the processing of personal data such as the use of new or changing technology.

19.3 A DPIA should include:

19.3.1 a description of the data processing and the purposes of the processing;

19.3.2 an assessment of the risk to individuals; and

19.3.3 the measures that are in place to, or are proposed to be put in place, to mitigate against any data breaches.

19.4 If you are unsure whether a DPIA is required or require further guidance on how to conduct a DPIA then please contact the GDPO.

20. DIRECT MARKETING

20.1 Consent is required for electronic direct marketing. The GDPR specifically prohibits pre-ticked opt-in boxes and therefore such methods should not be used as a manner of obtaining consent.

20.2 The right to object to direct marketing must be explicitly offered to the data subject. A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

21. SHARING PERSONAL DATA

21.1 Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

21.2 You may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information.

21.3 You may only share the personal data we hold with third parties, such as our service providers, if:

21.3.1 they have a need to know the information for the purposes of providing the contracted services;
21.3.2 sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;
21.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
21.3.4 the transfer complies with any applicable cross-border transfer restrictions; and
21.3.5 a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

21.4 If you are unsure whether you are able to transfer personal data to a third party then please contact the GDPO.

22. KEY CONTACTS

Group Data Protection Officer	Richard Zmuda	Group Company Secretary richard.zmuda@corservltd.co.uk
Corserv Limited	Rachel Siviter	Group Head of Business Systems rachel.siviter@corservltd.co.uk
Cornwall Airport Ltd	Matt Mitchell	Senior Finance & Data Analyst mjmitchell@cornwallairportnewquay.com
Cornwall Development Company	Nicky Pooley	Head of Corporate Services nicky.pooley@cornwalldevelopmentcompany.co.uk
Cornwall Housing Ltd	Alexandra Morgan-Thompson	Business Improvement Team alexandra.morgan-thompson@cornwallhousing.org.uk
Cormac Solutions Ltd Cormac Contracting Ltd	Kim Mundy	Policy Lead kim.mundy@corservltd.co.uk
Via East Midlands Limited	Sally Smith	Head of HR Sally.smith@viaem.co.uk

Document information

Contacts

Policy prepared by Company Secretariat Office, 1/11/2018

Further information

Further information regarding this policy can be obtained from the Company Secretariat Office.

Alternative formats

If you would like this information in another format please contact the Company Secretariat Office.

Please consider the environment. Only print this document if it cannot be sent electronically.

Version History			
Date	**Version**	**Author/Editor**	**Comments**
1/11/2018	v1.0	Jessica Riches	First draft for consultation.

Document retention	
Document retention period	5 years in hard and electronic copies.