Blackthorn

GDPR Transparency Notice
Blackthorn GRC Limited

REF: BT-S190319-01

Date: Feb 2022

Version: 1.2

UNCLASSIFIED

Document Control

Document Control	
Document Name:	GDPR Transparency Notice
Version Number:	1.2
Version Date:	21 Feb 2022
Status:	Issued
Document Author:	Nigel Adcock
Document Owner:	Nigel Adcock
Approved by:	Ian Hardman

Version Control

Version	Date	Author	Comments/ Amendments
0.1/0.2	19 Mar 2019	NA	First draft.
1.0	21 Mar 2019	NA	First formal release.
1.1	25 Mar 2019	NA	Minor update.
1.1a	19 Feb 2021	IH	Formal Record of Review
1.2	21 Feb 2022	IH	Added Ofgem 2022 Review and Approval

Distribution

Company/Dept.	Role	Name
Blackthorn GRC - Library	--	--

Approval

21/02/2022

X

Ian Hardman
Director

Confidentiality

This document is the property of Blackthorn GRC Limited and is issued for the information of such persons strictly on a need to know basis congruent with their official duties.

Any person finding this document should hand it into a Police Station for the safe return to Blackthorn GRC Limited, Victoria Plaza, Floor 3, Suite 3.22, 111 Buckingham Palace Road, London SW1W 0SR, with particulars of how and where found.

No part may be reproduced or used except as authorised by contract or other written permission.

When released outside of Government, the person to whom this document is trusted in confidence, is personally responsible, within the provisions of the Official Secrets Act 1911 to 1989, for its safe custody and for protecting the confidentiality of the information it contains which should only be disclosed to authorised third parties.

© Blackthorn GRC Ltd. 2022

1 Introduction

1.1 Purpose

This document sets out how we (Blackthorn GRC Ltd.) use personal data, as required by General Data Protection Regulation (GDPR).

It includes a Register of Processing Activities detailing processing activity by client, with confirmation of how we use and store personal data and a citizens' rights in respect of transparency, access, portability, processing, objection and erasure. For more information on citizen rights, please refer to the Information Commissioner's Office Website: https://ico.org.uk/.

1.2 Processor

GDPR makes a clear distinction between organisations functioning as a **data controller** and those acting as a **data processor**. Data controllers must exercise overall control over the purpose for which, and manner in which, personal data is processed. A data processor is any organisation that processes data on behalf of a data controller. All such processing must comply with clearly stated obligations, as set out by the data controller[1].

Blackthorn GRC has been contracted by some of its customers to undertake the processing of their data. This arises where Blackthorn GRC hosts one or more software products (e.g. Incident Management) for a customer and delivers operational capability as an on-line, on-demand subscription service. Through this channel, Blackthorn GRC might be the implicit custodian of personal data and, therefore, must comply with GDPR and discharge its contractual obligations as data processor, acting only on a lawful basis (i.e. complaint with the requirements of GDPR and UK law).

Where Blackthorn GRC provides a hosted service, Blackthorn GRC is the **data *processor*** for all processing of personal data, and our customer the ***data controller*** responsible for defining the nature of the processing. To deliver cloud hosted services, Blackthorn engages a with a small number of carefully selected sub-contractors who undertake specific data processing activities on Blackthorn's behalf. Blackthorn's sub-contractors are listed below:

a. UK Cloud: provision of a secure, UK-based data centre environment built to provide cloud services to the public sector.

b. Microsoft: provision of a secure, global network of tools and frameworks for hosting solutions. Blackthorn only uses data-centres located in London and Cardiff.

Our subcontractors are only engaged under formal contract agreements which formalise specific information security and data protection activities and controls. Where information security and data protection activities are observed but cannot be formally assured (i.e. though audit or other measures) Blackthorn GRC applies full database encryption to minimise the risk of data compromise.

Blackthorn GRC does not use personal data for any purposes other than that stipulated by the relevant ***data controller***. We do not use personal data for marketing and promotion activities, nor share personal data with anyone other than the recipients explicitly identified in the data processing specification supplied by our customers.

Blackthorn GRC is registered with the ICO as required by Data Protection Legislation.

Our data controller is Nigel Adcock whose duties include monitoring compliance with GDPR and advising the organisation on data protection obligations. He can be contacted at mailto:contact@blackthorn.com.

[1] On the proviso that such stated obligations do not contravene UK law.

1.3 Sub-processor

As the designer and vendor of software solutions, Blackthorn GRC has an obligation to provide customers with software maintenance and support. The provision of such support sometime necessitates access and visibility of client data, and potentially data of a personal nature. For example, a support ticket might be accompanied by files intended to illustrate a specific issue and these files could potentially contain information of a sensitive and/or personal nature. Similarly, the delivery of support might necessitate temporary access to a customer's Production environment and live data or access to a copy of production data enable user acceptance testing.

In such cases, Blackthorn GRC has no explicit data processing responsibility, but as a sub-contractor to the data processor (customer) Blackthorn GRC has a duty to provide such support in line with and compliant to GDPR. Whilst Blackthorn GRC will endeavour to operate in a lawful manner and in accordance with GDPR, it is our customer's responsibility to detail the processes that Blackthorn GRC should observe in the delivery of support in order that our actions do not frustrate their observance of the GDPR regulation.

1.4 Individual's Right to Object Under Data Protection Laws

UK Data Protection laws give UK citizens a number of rights regarding the handling, use and accuracy of their personal data. All such rights should be exercised through the appropriate Data Controller, details of which can be found in our Register of Processing Activities, below.

1.5 Contact

This you have any questions regarding you rights in relation to our processing of personal data, or the nature of the data processing we undertake for customers, we will respond directly, if within our authority, or refer your enquiry on to the relevant data processor. Alternatively, you can approach the relevant data controller directly.

Access request enquiries and any other enquiries relating to our Data Processing activities should be directed towards:

Data Protection Officer
Blackthorn GRC Limited
ONE Croydon, Suite 6-03, Floor 11
12-16 Addiscombe Road
Croydon
CR0 0XT
0208 123 7989

Annex A: Register of Processing Activities

Department of Health & Social Care: Injury Cost Recovery Admission Verification Information

Summary

Why and how we process your data in the Injury Cost Recovery admission verification system

Data Controller	Department of Health and Social Care (DHSC).
How is the information used by Department of Health	Treatment costs recovered from NHS patients who are also the beneficiaries of personal injury insurance.
How we use the information (Processing Activities)	Patient / hospital admission details received from DWP are provided to Trust hospitals for verification, then returned to DWP. Payment information circulated monthly to Trust hospitals.
Legal basis for processing data	The Health and Social Care (Community Health and Standards) Act 2003 gives the Department of Health legislative powers to require information from insurers and hospitals, in respect of chargeable personal injury related NHS treatment, and to exchange this with DWP.
Recipients of data	Department of Work & Pensions.
Is data transferred outside UK?	Data processed in UK sovereign datacentres. In returning information to DWP, encrypted data is sent to EU datacentres.
How long is data kept	As specified by DHSC ICR Data Retention Policy. Data retained while Individual claims remain open. Personal data redacted 3 months after claims paid or withdrawn. No data retained beyond 14 months, unless claim ongoing.
Your rights	Refer DHSC Privacy Notice available here .

CV Check Ltd: Pre-employment Screening Case Information

Summary

Why and how we process your data in the Pre-Employment Screening Case Management System

Data Controller	CV Check Limited.
How data is used by CV Check Limited	Data shared with national and international agencies (e.g. policy, government departments) past employers, and other reputable organisations to verify accuracy, uncover convictions and other dishonourable behaviour.
How we use the information (Processing Activities)	Information shared with 3rd-parties according to the specific requirements of the selected pre-screening, verification or search service. Creation of management reports, client reports and billing instructions. Further details are available here.
Legal basis for processing data	Candidate's consent and consent of parties engaged in the conduct of pre-screening operations.
Recipients of data	CV Check Ltd.
Is data transferred outside UK?	No
How long is data kept	Per engagement, 3 years from date of payment. Personal data, with exception of candidate name, redacted 6 months after date of payment. Further details are available here.
Your rights	Refer CV Check Ltd. Privacy Policy available here.

Office of Gas & Electricity Markets (Ofgem): Blackthorn Audit Portal

Summary

Why and how we process your data in the Blackthorn Audit Portal system

Data Controller	Office of Gas & Electricity Markets (Ofgem).
How is the information used by Ofgem	Assess the validity of continued membership of the Renewable Obligations Scheme and Domestic Renewable Heating Incentive.
How we use the information (Processing Activities)	Ofgem and contracted Ofgem on site auditors gather information on your appliances to assess the compliance of the application. Information may also be used to identify trends in applications.
Legal basis for processing data	• Domestic Renewable Heat Incentive Regulations 2014 (as amended) • The Renewables Obligation Order 2015 • Gas Act 1986 • Electricity Act 1989 • Utilities Act 2000 … plus, others. Please see the following for a full list: https://www.ofgem.gov.uk/publications/domestic-renewable-heat-incentive-privacy-notice https://www.ofgem.gov.uk/publications/domestic-renewable-heat-incentive-privacy-notice
Recipients of data	Office of Gas & Electricity Markets (Ofgem).
Is data transferred outside UK?	No. However, we will email you details of application to your specified email addresses that may be outside the UK.
How long is data kept	As specified by Ofgem privacy notice For the duration of the relevant scheme, and for a period of 6 years thereafter.
Your rights	Refer DHSC Privacy Notice available at https://www.ofgem.gov.uk/publications/renewable-electricity-schemes-privacy-notice https://www.ofgem.gov.uk/publications/domestic-renewable-heat-incentive-privacy-notice