UK General Data Protection Regulation Policy (GDPR)

Policy information		
Heading		**Information**
Organisation		Cava Security Services Ltd ICO Number **Z2805371**
Scope of policy		This policy applies to: • The Head office of Cava Security Services Ltd. • Its branches and regions. • Cava Security Training Centre. • All staff operating on behalf of Cava Security Services. It applies to payroll staff, sub-contractors, and 3rd Party Suppliers (sub processors).
Policy operational date		25 March 2022
Policy prepared by		Mal Ullah DPO and Richard Payton MD.
Date approved by Board/ Management Committee		Review minutes January 2022
Policy review date		15 March 2024

Introduction		
Heading		**Information**
Purpose of policy		The purpose of this policy is to enable Cava Security Services to: • comply with the law in respect of the data it holds about individuals. • follow good practice of the General Data Protection Regulation. • protect Cava Security Services customers, staff, and Group connections • protect the organisation from the consequences of a breach of its responsibilities.
Brief introduction to General Data Protection Regulation (EU) 2016/679		EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. In practice it provides a way for individuals to control information about themselves. Most of the Act does not apply to domestic use,[1] for example keeping a personal address book. Anyone holding personal data for other purposes is legally obliged to comply with this Act, subject to some exemptions. The Act defines eight **data protection principles**. It also requires companies and individuals to keep personal information to themselves.

Data Protection Principles		Everyone who is responsible for using data has to follow strict rules called 'data protection principles. They must make sure the information is: • used fairly and lawfully • used for limited, specifically stated purposes • used in a way that is adequate, relevant and not excessive • accurate • kept for no longer than is absolutely necessary • handled according to people's data protection rights • kept safe and secure • not transferred outside the UK without adequate protection
Personal data		This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the Data Protection Act, by virtue of not meeting the strict definition of 'data' in the Act.

Policy statement		Cava Security Services will: • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently Cava Security Services recognises that its first priority under GDPR t is to avoid causing harm to individuals. In the main this means: • keeping information securely in the right hands, and • holding good quality information. Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, Cava Security Services will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used and making them aware they can opt out allowing Cava Security Services to continue using the data previously authorised to use for the specific scope it was intended for at any time.
Key risks		Cava Security Services has identified the following potential key risks, which this policy is designed to address: • Breach of confidentiality (information being given out inappropriately) — especially at branch level. • Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed • Failure to offer choice about data use when appropriate • Breach of security by allowing unauthorised access - especially at branch level. • Failure to establish efficient systems of managing changes to branch managers leading to personal data being not up to date. • Harm to individuals if personal data is not up to date • Insufficient clarity about the way staff or subcontractor personal data is being used e.g. given out to general public. • Failure to offer choices about use of contact details for staff • Data Processor contracts

Responsibilities		
Heading		**Information**
Shareholders		The shareholders recognise its overall responsibility for ensuring that Cava Security Services complies with its legal obligations.
Data Protection Officer		The Data Protection Controller is currently Mal Ullah, with the following responsibilities: • Briefing the board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Team/Department managers		Each team or department where personal data is handled will follow head office procedures (including induction and training) to ensure that good Data Protection practice is established and followed. Each Branch Manager is responsible their branch's compliance with this policy and supporting guidance.
Staff & Subcontractors		All staff and sub-contractors are required to read, understand, and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
Enforcement		Significant breaches of this policy will be handled under the Companies disciplinary procedures.

Confidentiality		
Heading		**Information**
Extension to Scope		Because confidentiality applies to a much wider range of information than Data Protection, Cava Security Services has a separate Confidentiality Policy.

Communication with Data Subjects		Cava Security Services have a privacy statement for Data Subjects, setting out how their information will be used. This will be available on request, and a version of this statement will also be used on the Cava Security Services web site: http://www.cavaguard.co.uk/privacy-policy/
Communication with staff		Staff, subcontractors will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities. (See Appendix B.)
Authorisation for disclosures not directly related to the reason why data is held		Where anyone within Cava Security Services feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done with the authorisation of the Data Protection Officer. All such disclosures will be documented as outlined to Human Resources.

Security		
Heading		**Information**
Security of information		This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.
Specific risks		Cava Security Services has identified the following risks: • Information passing between the head office and branches, or post offices could go astray or be misdirected. • Staff or volunteers with access to personal information could misuse it. • Staff could continue to be sent information after they have stopped working for Cava Security Services if their records are not updated promptly. • Poor web site security might give a means of access to information about individuals once individual details are made accessible online. • Staff may be tricked into giving away information, either about colleagues, especially over the phone, or through “social networks”.
Setting security levels		Access to information on the main computer systems will be controlled by Colin Harris (Data Controller) Then in his absence. Mal Ullah DPO or Jamie Whitby Operations Supervisors (Data Processor) in their absence Steve Slade Control Room Supervisor (Data Processors). Access to certain HR files/forms to Steve Slade Control Room & Mal Ullah (Compliance Director). The greater the consequences of a breach of confidentiality, the tighter the security will be.
Security measures		• Customer data will be kept in a sterile area at: Head Office: 7 The Oaks, Clews Road, Redditch, B98 7ST Control Room: 7 The Oaks, Clews Road, Redditch, B98 7ST Training Centre, Unit 44, IMMEX Business centre, Redditch, B98 0RE • Staff data will be kept in a sterile area at head office and within data protection lockable cabinets with authorised access at branches.
Business continuity		Cava Security Services have a business continuity statement, setting out how Cava Security Services back up will provide continuity for the customers and staff including emergency planning. This will be available on request.
Personal safety		Lone worker monitoring will be provided to all staff and information about them including medical information will be screened to the personnel managing said staff.

Data recording and storage		
Heading		**Information**
Accuracy		Cava Security Services is moving towards a single database holding basic information about all customers and staff. Branches will for the time being, however, continue to hold separate registers of their staff. Cava Security Services will regularly review its procedures for ensuring that its records remain accurate and consistent and, in particular: • IT systems will be designed, where possible, to encourage and facilitate the entry of accurate data. • Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets. • Effective procedures will be in place so that all relevant systems are updated when information about any individual changes. • Staff or volunteers who keep more detailed information about individuals will be given additional guidance on accuracy in record keeping.
Updating		Data will be updated annually for customers who will receive a letter with their renewal invoice however contractually the customers are to furnish Cava Security Services with this information as and when it changes. This is normally completed in an email authoring changes to assignments.
Storage		Data is either on main computer within the sterile area of head office or filed (hard copy) within same area.

Retention periods		Cava Security Services will establish retention periods for at least the following categories of data: • Customer-permanent while live • Staff –permanent while employed • Sub-Contractors- permanent while supplying services.
Archiving		Archived paper records of members are stored securely on site and on cloud.

Subject access		
Heading		**Information**
Responsibility		Any subject access requests will be handled by the Data Protection Officer.
Procedure for making request		Subject access requests must be in writing. All managers and staff are required to pass on anything which might be a subject access request to the Data Protection Officer without delay. All those making a subject access request will be asked to identify any branches managers or staff who may also hold information about them, so that this data can be retrieved.
Provision for verifying identity		Where the individual making a subject access, request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.
Charging		When an individual is making a subject access request depending on the information requested is dependent on a charge levied against this request, no charge will be made for this- See privacy statement.
Procedure for granting access		The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

Transparency		
Heading		**Information**
Commitment		Cava Security Services is committed to ensuring that in principle Data Subjects are aware that their data is being processed and • for what purpose it is being processed. • what types of disclosure are likely; and • how to exercise their rights in relation to the data.

Procedure		Data Subjects will generally be informed in the following ways: • Managers & Staff: in the staff handbook • Customers: in the welcome pack • Company webpage Standard statements will be provided to staff at head office and to branches for use on forms where data is collected. Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Consent		
Heading		**Information**
Underlying principles		Consent will normally not be sought for most processing of information about **staff** and **customers**, with the following exceptions: • Staff details will only be disclosed for purposes unrelated to their work for Cava Security Services (e.g., financial) with their consent. • Managers, Sales, or other staff working from home, will be given the choice over which contact details are to be made public. Information about **sub-contractors** will be made public according to their role, and consent will be sought for (a) the means of contact they prefer to be made public, and (b) any publication of information which is not essential for their role. Information about **customers** will only be made public with their consent. (This includes photographs.) 'Sensitive' data about staff & customers if applicable (including health information) will be held only with the knowledge and consent of the individual.
Forms of consent		Consent must be given in writing email will be sufficient, verbal will not be considered.
Opting out		Customers may opt out from data being available in different ways (e.g., not to receive direct marketing) this will be consented by the above manner.
Withdrawing consent		The organisation may wish to acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct marketing		
Heading		**Information**
Underlying principles		Cava Security Services will treat the following unsolicited direct communication with individuals as marketing: • seeking donations and other financial support. • promoting any Cava Security Services. • promoting branch events. • promoting sponsored events and other fundraising exercises. • marketing the services of Cava Security Services. • marketing on behalf of any other external company or voluntary organisation.
Opting out		Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Cava Security Services marketing.

Sharing lists		Cava Security Services has the policy of sharing lists (or carrying out joint or reciprocal mailings) only on an occasional and tightly controlled basis. Details will only be used for any of these purposes where the Data Subject has been informed of this possibility, along with an option to opt out, and has not exercised this option. Please also see privacy policy- http://www.cavaguard.co.uk/privacy-policy/ Cava Security Services undertakes to obtain external lists only where it can be guaranteed that the list is up to date and those on the list have been given an opportunity to opt out.
Electronic contact		Cava Security Services will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the purchased telephone data. Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Staff training & acceptance of responsibilities		
Heading		**Information**
Documentation		Information for Staff is contained in the staff handbook. Staff GDPR e- leaning training, staff above supervisor level GDPR for managers/supervisors e-leaning training, refresher training annually. Information for branches is contained in branch operational manual.
Other related policies		Quality Management System ISO 9001:2015. CCTV Policy, Information Security Policy, Cyber Security Policy, Laptop Policy, Desk Tidy Policy, Cava Security Data Protection and Security Policy.
Induction		All staff who have access to any kind of personal data will have their responsibilities outlined during their induction procedures. Data Protection will be included in Business training for branch managers
Continuing training		Cava Security Services will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.
Procedure for staff signifying acceptance of policy		See Appendix B

Policy review		
Heading		**Information**
Responsibility		The next policy review will be audited, approved, and amended if required by Mal Ullah Compliance Director
Procedure		Richard Payton and Technical Director will be consulted in review.
Timing		The review will be completed in August 2023

Changes to the Policy	**Information change**	**Date & Version Number**
Responsibility person making the changes will be the DPO Mal Ullah	**(Uk) added to GDPR**	**V2 15/0/2022**
Procedure, consultation with the Data Controllers and senior management	**No changes**	**V4 reviewed 15/03/23**

Notes

Data Controller

The Data Controller is the legal 'person' responsible for complying with the UK GDPR. It will almost always be the organisation, not an individual staff member or volunteer. Separate organisations (for example a charity and its trading company) are separate Data Controllers. Where organisations work in close partnership it may not be easy to identify the Data Controller. If in doubt, seek guidance from the Information Commissioner.

Data Processor

When work is outsourced, which involves the contracting organisation in having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of Data Protection brought about by the Data Processor.

Fair processing conditions

Schedule 2 six conditions of the GDPR, at least one of which must be met, in order for any use of personal data to be fair. These are (in brief):

- With consent of the Data Subject
- If it is necessary for a contract involving the Data Subject
- To meet a legal obligation
- To protect the Data Subject's 'vital interests'
- In connection with government or other public functions
- In the Data Controller's 'legitimate interests' provided the Data Subject's interests are not infringed

Subject access

Individuals have a right to know what information is being held about them. The basic provision is that, in response to a valid request (including the fee, if required), the Data Controller must provide a permanent, intelligible copy of all the personal data about that Data Subject held at the time the application was made. The Data Controller may negotiate with the Data Subject to provide a more limited range of data (or may choose to provide more), and certain data may be withheld. This includes some third-party material, especially if any duty of confidentiality is owed to the third party, and limited amounts of other material. ("Third Party" means either that the data is about someone else, or someone else is the source.)

Appendix: Privacy statement

When you request information from Cava Security Services, sign up to any of our services, Cava Security Services obtains information about you. This statement explains how we look after that information and what we do with it.

We have a legal duty under the General Data Protection Regulation UK GDPR to prevent your information falling into the wrong hands. We must also ensure that the data we hold is accurate, adequate, relevant, not excessive, and lawfully used.

Normally the only information we hold comes directly from you. Whenever we collect information from you, we will make it clear which information is required in order to provide you with the information, service, or goods you need. You do not have to provide us with any additional information unless you choose to. We store your information securely on our computer system, we restrict access to those who have a need to know, and we train our staff in handling the information securely.

Most of our services are delivered through our branches. We will pass your contact details to your local branch, so that they can let you know what activities are available in your area. We will also pass your details to the professional manager/member of staff providing that service. The branch or manager or security personnel may hold additional information about your participation in local activities.

We would also like to contact you in future to tell you about other services we provide, and ways in which you might like to support Cava Security Services. You have the right to ask us not to contact you in this way. We will always aim to provide a clear method for you to opt out. You can also contact us directly at any time to tell us not to send you any future marketing material.

You have the right to a copy of all the information we hold about you (apart from a very few things which we may be obliged to withhold because they concern other people as well as you). To obtain a copy, either ask for an application form to be sent to you or write to the Data Protection Officer at Cava Security Services. There will be no charge for reasonably requested data. We aim to reply as promptly as we can and, in any case, within the legal maximum of 40 days.

Cava Security Services does not install cookies onto our website to enable us to track your IP address for marketing purposes.

1. **Can Cava Security Services contact you in the future regarding other services that we can offer, the main scope of which is: Site Security, Patrolling, open & Close, event Security, CCTV Monitoring, Key Holding and or alarm response services or lone worker monitoring and vehicle tracking YES/NO**

2. **You understand that we will use any data you provide us with legally and it will only be passed on to the law enforcement agency if required to and our approved GDPR compliant HR and Credit Agency supporting companies, and that both parties are responsible and have an obligation to keep the data accurate YES/NO**

3. **You know you have a right to ask Cava Security Services Ltd in writing/email to stop using your data at any time YES/NO**

You understand the Privacy Statement, are authorised to have answered the 3 questions above and to sign this privacy statement: - Signature: _____

Name: _____ Position in the company (if applicable): _____Date: _____

Appendix B: Confidentiality statement for staff

When working for Cava Security Services Ltd, you will often need to have access to confidential information which may include, for example:

- Personal information about individuals who are supporters or otherwise involved in the activities organised by Cava Security Services Ltd.
- Information about the internal business of Cava Security Services Ltd.
- Personal information about colleagues working for Cava Security Services Ltd.
- Customer's data, including but not exhaustive; alarm codes, access codes, contact information, sensitive area information.

Cava Security Services Ltd is committed to keeping this information confidential, in order to protect people and Cava Security Services Ltd itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must assume that information is confidential unless you know that it is intended by Cava Security Services Ltd to be made public. Passing information between a branch and the Head office, or *vice versa* does not count as making it public, but passing information to another organisation does count.

You must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- not compromise or seek to evade security measures (including computer passwords);
- be particularly careful when sending information between the UK office and branches.
- not gossip about confidential information, either with colleagues or people outside Cava Security Services Ltd.
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with an appropriate person whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for Cava Security Services Ltd.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: **Date:**