INFORMATION PRIVACY MANUAL

Bell Equipment Ltd

CONTENTS

INTRODUCTION

In May 2018, the European Union's General Data Protection Regulation became enforceable for all Union Members and all persons, bodies, entities and organisations processing the personal information of citizens of the Member States. The Regulation aims to protect the privacy interests of European citizens and regulate the processing and use of personal information. The Regulation requires data controllers to comply with the certain conditions for lawful processing of personal information, these conditions are briefly outlined below.

- **Lawfulness, Fairness and Transparency**
  Personal Information must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject
- **Purpose Limitation**
  Personal Information must be collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Data Minimization**
  Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy**
  Personal Information must be accurate and, where necessary, kept up-to-date. Reasonable steps must be taken to ensure that the Personal Information which is inaccurate, is erased or rectified in a reasonable manner
- **Storage Period Limitation**
  Personal Information must be kept for no longer than is necessary for the purposes for which the Personal Information is processed
- **Integrity and Confidentiality**
  Appropriate security, technical and organisational measures should be implemented in a manner that ensures the security of the Personal Information and the protection against accidental or unlawful destruction, loss, alteration, unauthorised access to or disclosure of the Personal Information.
- **Accountability**
  Data Controllers must be responsible for and be able to demonstrate compliance with the principles outlined above.

This Manual is likewise created to demonstrate the Company's compliance with the above conditions for the lawful processing of Personal Information, as well as to give effect to the rights of the data subjects from which we process Personal Information.

SCOPE OF THE MANUAL

Bell Equipment Ltd is a holding company of 3 European subsidiary companies in France, Germany and the UK, involved in the manufacturing and distribution of heavy earth moving vehicles. Technical Information Security measures for the Bell Equipment Group is controlled, implemented and maintained by the IT Services Department at the Group's head office in Richards Bay, South Africa. All European subsidiary companies of the Bell Equipment Group are required to comply with GDPR, in cooperation with the Group's IT Services Department to ensure that Personal Information is processed, lawfully, fairly and in a transparent manner, giving effect to the rights of the Data Subjects concerned and maintaining the confidentiality, integrity and availability of the Information collected.

THE COLLECTION OF PERSONAL INFORMATION

THE CATEGORIES OF PERSONAL INFORMATION COLLECTED BY THE COMPANY:

- Employee Information
- Customer Information
- Information of representatives of Dealers the Company contracts with
- Information of representatives of Service Providers and Suppliers that the Company Contracts with

THE PERSONAL INFORMATION COLLECTED:

Personal Information Collected in respect of Customers, Suppliers, Dealers and Service Providers:

- Name and Surname
- Business address
- Business telephone and fax numbers
- Business email address
- Banking details
- Correspondence with and within the Company

Personal Information Collected in respect of Employees only:

- Personal Contact details such as name, title, address, telephone numbers, email addresses
- Identity Number/Social Security Number
- Date of birth
- Gender
- Copy of driving licence, passport, Identity Document, Marriage Certificate, Decree Absolute
- Marital status and dependants
- Next of kin, emergency contact number and death benefit nominee(s) information
- Bank Account Details, Payroll Records, Tax Administration Information
- Salary and Compensation history
- Annual, sick, maternity, paternity leave, family responsibility leave
- Information relating to pension and benefits
- Recruitment information (information included in your CV, cover letter as part of the application process
- Copies of work permit or visa or immigration status, if applicable
- Full employment records (contract, terms and conditions of employment, job titles, work history, working hours, promotion, absences, attendances, training records, starting date and leaving date of employment, location of employment)
- Performance and appraisal information
- Disciplinary and grievance information
- Secondary employment information
- Access card records

- Information about your use of the Company's information and communication systems
- Photographs
- Injury at the workplace and third party accident information
- Employee screening information
- Video Surveillance

THE PURPOSES FOR WHICH THE INFORMATION IS COLLECTED:

- The fulfilment of contractual obligations between the data subject and the Company or the Company and third parties;
- We require your contact details to communicate with data subjects and with their consent, provide them marketing material in areas of their interest;
- Ascertaining the Identity of the data subject
- Communicating with the data subject
- Making a decision about recruitment of employees
- Determining the terms and conditions employment for our employees
- Determining whether a prospective employee is legally entitled to work in the country
- Paying salaries and deducting tax and national insurance contributions
- Liaising with pension providers of employees
- Business management planning, including accounting and auditing
- Conducting performance reviews and compensation
- Assessing qualifications for a particular job, task or promotion
- Gathering evidence and any other steps relating to possible grievance or disciplinary matters and associated hearings
- Making decisions about an employees continued employment
- Dealing with legal disputes involving
- Determining fitness to work of employees and complying with health and safety obligations
- To provide access to and monitor business and personal use of our information and communication systems
- To ensure network and information security and preventing access to our network and communication systems
- Ensuring employment equity
- Access control and security purposes

SPECIAL CATEGORIES OF PERSONAL INFORMATION

Although the processing of personal information is generally prohibited, the Company is allowed to processes your special personal information in the following circumstances:

- Where you have granted us consent to process your special personal information
- Processing is necessary for the purposes of carrying out the obligations and exercising your specific rights in the field of employment and social security

- The processing is necessary to protect your vital interests or another person where you are physically or legally incapable of consenting
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of your working capacity

TYPES OF SPECIAL PERSONAL INFORMATION WE COLLECT FROM YOU

- Race or ethnicity
- Trade union membership
- Medical records collected at the on-site clinic, Information about your health, including any medical condition.
- Biometric data

PURPOSES FOR WHICH WE COLLECT YOUR SPECIAL PERSONAL INFORMATION

- We may process information relating to leave of absence, which may relate to illness, to comply with employment and other laws
- We may process information regarding your physical or mental health or disability status to assess your fitness to work and protect your health and safety in the workplace
- We may process information about your race or ethnic origin to comply with legal obligations regarding employment equity
- We may process your personal information relating to trade union membership in order to pay union premiums and comply with labour law obligations

STORAGE OF PERSONAL INFORMATION:

Information is stored in the following formats:

- Electronic documents (backed up on the network or cloud storage)
- Paper documents in a filing system
- In specific books designated by the Company
- Applications (backed up on the server or cloud)

THE PERIOD FOR WHICH THE INFORMATION IS STORED:

Personal information of representatives of the Dealers, Suppliers, Service Providers and Customers are retained for as long as the relationship requires. Once a Dealer, Supplier, Service Provider or Customer no longer wishes to conduct business with the Company, the information will be archived and no longer used by the Company and may be deleted upon their request.

Where information is collected in accordance with labour law, the legislation usually specifies a retention period for employee records. Bell Equipment operations in various countries will be required to comply with the retention periods in their respective countries. Where there is no specific retention period, the company will follow industry best practices with regards to retention of employee personal information.

INFORMATION TRANSFERRED TO THIRD PARTIES:

- Employee information is transferred to tax authorities and other labour authorities in accordance with tax administration and labour regulations
- Certain employee information may be transferred to an accounting/payroll service provider
- Basic employee information such as name, surname, email address and job description is saved on the email client used by the Bell Equipment Group and is accessible by all employees of the Bell Equipment Group with email access.
- Employee payroll information is transferred to the Group's Head Office in South Africa
- Customer Data is saved on the Group's CRM system and can be accessed by all employees of the Bell Equipment Group with access to the CRM system.

CROSS-BORDER TRANSFERS OF EMPLOYEE PERSONAL INFORMATION

Personal Information collected from the Bell Equipment operations in Europe, Africa and North America is often shared with our head office in South Africa as part of regular reporting and analytic activities, hosting of data and general administration purposes. All information stored on the Bell Equipment Network is hosted by our head office in South Africa. Transfers of personal information takes place in accordance with our Cross-border Transfer of Personal Information Policy, which ensures that personal information is adequately protected by our head office and the methods of transfer used by the sending party is secure. Security of personal information is discussed further below.

ACCURACY OF INFORMATION

- Information collected from the data subject is verified by the data subject and data subjects are encouraged to inform the Company of changes in their personal information.

SECURITY MEASURES IMPLEMENTED BY THE COMPANY

OPERATIONAL MEASURES

PERSONS RESPONSIBLE FOR THE ENSURING THE PROTECTION OF PERSONAL INFORMATION

- **IT Operations Manager:** responsible for protecting the Company's information by designing, implementing and enforcing security controls and safeguards.
- **Information Security Analysts:** Monitor computer networks for security issues. Investigate security breaches and other cyber security incidents.
  Install security measures and operate software to protect systems and information infrastructure, including firewalls and data encryption programs.
- **Compliance Officers:** Develops initiates, maintains, and revises policies and procedures for the Information Security, Business Continuity and Quality assurance operation of the IT Compliance Program and its related activities to prevent illegal or improper conduct.

TRAINING

The Company has developed a Cybersecurity Awareness Training Course for end-users throughout the Bell Equipment Group.

IMPACT ASSESSMENTS

Effectiveness of security controls are measured annually during audit assessments.

POLICIES

Various policies assist with regulating the manner in which information is processed, handled and stored as well how access to confidential information is limited and controlled. The Company has implemented the following Information Security Policies:

- Information Security Policy
- Acceptable use Policy
- Information Classification Policy
- Information Transfer Policy
- Account Management Policy
- Bring You Own Device Policy
- Clear Screen and Clear Desk Policy
- Disposal and Destruction Policy
- End-Point Security Standard
- General Data Protection Policy

DUTY OF CONFIDENTIALITY

Employees who have access to personal information processed by the company are required to sign a non-disclosure agreement. Likewise third parties who process personal information on the Company's behalf are required to conclude a Data Processing Agreement, stipulating how personal information should be processed, stored and handled, for the purpose of keeping personal information strictly private and confidential.

TECHNICAL AND PHYSICAL SECURITY MEASURES

FORMAT OF DATA

Personal Information is required to be stored in a password encrypted format and location in order to limit the accessibility of the information to authorised persons only. The Information Classification Policy stipulates how personal information should be handled.

ACCESS PROCEDURES

The Company follows an access control system on specific databases or software programmes, whereby access to certain information can be limited to authorised persons only, (ie. Persons who require access to personal information in order to carry out employment duties.) A manager would authorise an employee's access request based on his/her employment role. Access to the particular database or software programme is based on an authentication process. Once access is to the information is no longer necessary to his/her carry out employment duties, the access will be relinquished.

Personal information stored in files on a computer are password protected and only transferred to authorised persons who require the information to carry out employment duties.

PHYSICAL ACCESS PROCEDURES

Access to the main data centres are limited via an access card clock-in system. Access is granted to those employees who require the access as a part of their employment duties. A Data Centre Access Policy stipulates who has access to the data centres and how access is granted and monitored.

DISPOSAL AND DESTRUCTION OF INFORMATION

Once information is no longer needed, it must be destroyed or disposed of as stipulated in the Disposal and Destruction Policy.

PHYSICAL SECURITY OF INFORMATION ASSETS

Users are required to ensure that their information assets are kept safe at all times in accordance with the Acceptable Use Policy.

MONITORING OF SECURITY THREATS

The Information Security Analyst is responsible for continually monitoring security threats posed to the Company, taking measured to prevent threats and alerting the Company of potential security breaches.

SECURITY FEATURES ON SOFTWARE, APPLICATIONS AND ASSETS

Some of the security features employed by the Company include:

- Firewalls
- Threat Prevention
- Host Intrusion Prevention
- File and removable media encryption
- Full Disk Encryption
- Authentication systems
- VPN

BREACH AND SECURITY INCIDENTS

The Company implements a Security Incident Management Procedure regulating how security breaches should be handled. The Policy stipulates who is responsible for managing the incident, the measures which should be taken to prevent and minimize the occurrence of the incident, how the incident should be reported and who should be notified in the event of an incident. Incidents affecting the security of personal information must be reported to the relevant Supervisory Authority, within 72 hours, in accordance with the Contact with Authorities and Special Interest Groups Procedure.

INQUIRIES AND COMPLAINTS

GDPR stipulates certain rights which should be made enforceable for data subjects. Data subjects have the right to access a copy of their personal information records held by the Company and request that information be rectified or erased if incorrect or unnecessary. A data subject may also withdraw his/her consent to process his/her personal information and request that the Company stop processing his/her personal information.

DATA SUBJECT ACCESS REQUESTS

A data subject may request confirmation the following via the Data Subject Access Request Form:

- Whether the Company holds any personal data about them.
- A description of the data held about them and, if permissible and practical, a copy of the data.
- The purpose(s) for which that data is being processed, and from where it was received.
- Whether the information is being disclosed to anyone apart from the original recipient of the data; and if so, the identity of those recipients.
- The right of data portability. Data subjects can ask that their personal data be transferred to them or a third party in machine readable format (Word, PDF, etc.). However, such requests can only be fulfilled if the data in question is: 1) provided by the data subject to the Company, 2) is processed automatically and 3) is processed based on consent or fulfilment of a contract.
- Whether the data is being used to make automated decisions about the data subject, to be told what logic the system uses to make those decisions and to be able to request human intervention.

The Company must provide a response to data subjects requesting access to their data within 30 calendar days of receiving the Data Subject Access Request unless local legislation dictates otherwise.

An individual does not have the right to access information recorded about someone else, unless they are an authorized representative.

The Company is not required to respond to requests for information unless it is provided with sufficient details to enable the location of the information to be identified, and to satisfy itself as to the identity of the data subject making the request.

EXEMPTIONS

In principle, the Company will not normally disclose the following types of information in response to a Data Subject Access Request:

- Information about other people – A Data Subject Access Request may cover information which relates to an individual or individuals other than the data subject.

Access to such data will not be granted, unless the individuals involved consent to the disclosure of their data.

- Repeat requests – Where a similar or identical request in relation to the same data subject has previously been complied with within a reasonable time period, and where there is no significant change in personal data held in relation to that data subject, any further request made within a six month period of the original request will be considered a repeat request, and the Company will not normally provide a further copy of the same data
- Publicly available information – The Company is not required to provide copies of documents which are already in the public domain.
- Opinions given in confidence or protected by copyright law – The Company does not have to disclose personal data held in relation to a data subject that is in the form of an opinion given in confidence or protected by copyright law.
- Privileged documents – Any privileged information held by Company need not be disclosed in response to a DSAR. In general, privileged information includes any document which is confidential (e.g. a direct communication between a client and his/her lawyer) and is created for the purpose of obtaining or giving legal advice.

SUBMITTING A REQUEST

In order to enable the Company to respond to the Data Subject Access Requests in a timely manner, the data subject should:

- Submit his/her request using a Data Subject Access Request Form, provided in Annex 1 below, and
- Provide the Company with sufficient information to validate his/her identity (to ensure that the person requesting the information is the data subject or his/her authorized person.)

Data Subject Requests must be made to the Group Company Secretary, via the contact details provided in Annex 2 below.

DATA SUBJECT COMPLAINTS

In terms of Article 13 (2)(d) of the GDPR, the data subject must be informed of his/her right to lodge a complaint with the Supervisory Authority. Article 77 provides that every data subject shall have the right to lodge a complaint with the supervisory authority, in particular, in the Member State of his/her habitual residence, place of work or of the alleged infringement. Contact details of the relevant supervisory authorities are included in Annex 3 below.

EFFECTIVITY OF THE MANUAL

This Manual shall be effective from July 2019; and shall remain in effect until otherwise repealed. This Manual must be annually reviewed for compliance with the relevant data protection laws and kept up to date by the Company.

ANNEX 1: DATA SUBJECT ACCESS REQUEST FORM

You have the right to request for personal data we may hold about you. This is known as a Data Subject Access Request ("DSAR"). A data subject is an individual who is the subject of the personal data. If you wish to make a DSAR, please complete this form and return to us by post or email.

DATA SUBJECT'S PARTICULARS

Please enclose a copy of your Identity Document and proof of residential address with your request as proof of identity.

Full Name:	
Date of Birth:	
Physical Address;	
Telephone Number:	
Mobile Phone Number:	

DETAILS OF THE REQUEST

Provide a detailed description of the information you require:

CONFIRMATION OF IDENTITY OF DATA SUBJECT

I_____, confirm on the _____day of _____ 20__ that I am the Data Subject concerned and the personal information requested is my personal information.

_____

Signature

AUTHORISATION OF DATA SUBJECT'S REPRESENTATIVE (IF APPLICABLE)

I hereby grant _____ on the _____day of _____20___, my permission to make a request for access to my personal information on my behalf.

_____

Signature

PARTICULARS OF THE AUTHORISED REPRESENTATIVE (IF APPLICABLE)

Please enclose a copy of the Representative's Identity Document and proof of residential address with the request as proof of identity.

Full Name:	
Date of Birth:	
Physical Address;	
Telephone Number:	
Mobile Phone Number:	

I _____, confirm on the _____ day of _____ 20___ that I am the Data Subject's Representative.

_____

Signature

We will make every effort to process your data subject access request as quickly as possible within 30 calendar days. However, if you have any queries whilst your request is being processed, please do not hesitate to contact us.

ANNEX 2: CONTACT DETAILS

CONTACT DETAILS OF THE RESPONSIBLE OFFICERS

Group Company Secretary:

Diana McIlrath

Email: Diana.McIlrath@bellequipment.com

Telephone: +27(0)35 907 9716

IT Operations Manager:

Andre Neethling

Email: Andre.Neethling@bellequipment.com

Telephone: +27 (035) 907 9202

BELL EQUIPMENT LTD AND SUBSIDIARY COMPANIES

Within the European Union:

Bell Equipment (Deutschland) Gmbh

Bell France SAS

Bell Equipment UK Limited

Outside the European Union:

Bell Equipment Company South Africa (Pty) Ltd

Bell Equipment Sales South Africa Limited

Bell Equipment North America Inc

LLC Bell Equipment Russland

Bell Equipment Australia (Pty) Ltd

IA Bell Equipment Company Namibia (Pty) Ltd

Bell Equipment Company Swaziland (Pty) Ltd

Bell Equipment Zambia Ltd

CONTACT DETAILS OF THE SUPERVISORY AUTHORITIES WHERE WE PROCESS PERSONAL INFORMATION

France

Commission Nationale de l'Informatique et des Libertés - CNIL

8 rue Vivienne, CS 30223

F-75002 Paris, Cedex 02

Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

e-mail:

Website: **http://www.cnil.fr/**

Germany

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30

53117 Bonn

Tel. +49 228 997799 0; +49 228 81995 0

Fax +49 228 997799 550; +49 228 81995 550

e-mail: poststelle@bfdi.bund.de

Website: **http://www.bfdi.bund.de/**

United Kingdom

The Information Commissioner's Office

Water Lane, Wycliffe House

Wilmslow - Cheshire SK9 5AF

Tel. +44 1625 545 745

e-mail: international.team@ico.org.uk

Website: **https://ico.org.uk**

Russia

Roskomnadzor

Moscow, Moscow City, Russian Federation

Email: rsoc_in@rsoc.ru

Website: **eng.rkn.gov.ru/**

South Africa

Information Regulator

SALU Building, 316 Thabo Sehume Street, PRETORIA

Tel: 021 406 4818

Fax 086 500 3351

Email: inforeg@justice.gov.za

Website: **justice.gov.za/inforeg**