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.

DEFINTION

Consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data subject	means the persons to whom personal information relates
De-identify	In relations to personal information of a data subject, means to delete any information that: • Identifies the data subject, • Can be used or manipulated by a reasonably foreseeable method to identify the data subject, or • Can be linked be a reasonably foreseeable method to other information that identifies the data subject.
Direct Marketing	means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: • promoting or offering to supplying, in the ordinary course of business, any goods or services to the data subject, or • requesting the data subject to make a donation of any kind for any reason
Electronic communication	means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Filing system	means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria
Information Officer	In relation to a private body means the head of a private body as contemplated in Section 1, of the Promotion of Access to Information Act
Operator	means a persons who processes personal information for a responsible party in terms of a contract or mandate, without coming under the authority of that party
Person	means a natural person or a juristic person
Personal Information	Means information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person, including but not limited to: • Information relating to the race, gender, sex pregnancy, marital status, national, ethic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person, • Information relating to the education or the medical, financial, criminal or employment history of the person, • Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person,

	• the biometric information of the person, • the personal opinions, views or preferences of the person, • correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence. • the views or opinions of another individual about the person, and • the name of the person if it appears with other personal information relating to the person or it the disclosure of the name itself would reveal information about the person
Private Body	means: • a natural person who carries or has carried on any trade, business or profession, but only in such capacity, • a partnership which carries or has carried on any trade, business or profession, or • any form or existing juristic person but excludes a public body.
Record	means any recorded information: • regardless of form or medium, including any of the following: o Writing on any material, o Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored, o label, marking or other writing that identifies or describes anything of which it forms part, or which it is attached by any means, o book, map plan, graph or drawing, o photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced, • in the possession or under the control of a responsible party, • whether or not it was created by a responsible party, and • regardless of when it came into existence.
Responsible Party	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

THE COLLECTION OF PERSONAL INFORMATION

Bell Equipment Ltd processes personal information in terms of this policy when the company acts as a responsible party (we decide why and how to process the personal information). We take privacy seriously.

This policy (read with other notices given to individual data subjects) is our notice in terms of Section 18 of the Protection of Personal Information Act, 2013 (POPIA)

This policy describes what personal information we process, where we collect it, why we process it and the legal basis on which we do so and generally, how we do so.

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 of 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
- Determining fitness of employees to work 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 process 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 at 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 for personal information stored 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 an 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 measures 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 retains the responsibility to report any notification of security compromises as required by Section 22 of POPIA. 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.

INFORMATION VIA OUR WEBSITE AND SOCIAL MEDIA PLATFORMS

A data subject does not have to provide personal information to the Company when he/she visit the Company's website or communicates with us using a social media platform on which the Company has an account but the data subject can do so by:

- *sending an enquiry to us;*
- *subscribing to newsletters and marketing communication;*
- *registering for an event;*
- *applying for a job by emailing us or, where applicable, through our website.*

If the data subject provides the Company with personal information using the Company's website or when the data subject communicates with us using our social media accounts, the Company sources that information from them, with their consent and will only use it for the purpose for which they provide it.

The data subject email enquiries are held on the Company's email server, by the addressee and by anyone in our business to whom the addressee refers his/her email for a response. The data subject subscription and registrations are held by our marketing personnel. Job applications are held by human resources personnel and anyone whom our human resources personnel refer the application for consideration.

The Company uses the personal information that the data subject provides to us through our website or when communicating with the Company using our social media accounts:

- *for the purposes for which he/she provided it;*
- *to administer and improve our website;*
- *to improve our services;*
- *to communicate with us.*

INFORMATION RELATING TO JOB APPLICATIONS

The Company processes the personal information relating to the job applicants including names, contact details (including phone numbers, email and other addresses), education and employment history, race, gender and any other personal information included in the job application (Applicant Information).

The Company sources most of the Applicant Information from the job applicant in person, by email or, where applicable, through our website. We may also source Applicant Information from recruitment agents and websites such as LinkedIn, from references, public records and licenced databases.

The Company processes Applicant Information to consider and deal with the job applications and so that we can contact applicants about possible job opportunities.

The legal basis on which the Company processes the Applicant Information is consent or our legitimate interests in recruiting employees for our business.

SUPPLIER INFORMATION

The Company processes personal information relating to potential actual suppliers of goods and services including names, identity, passport or registration numbers, contact information (including phone numbers, email and other addresses), VAT numbers, bank account details (Supplier Information).

The Company usually sources the supplier information directly from our potential or actual suppliers but we may source it from quotations, adverts, references or other suppliers.

The Company processes supplier information in relation to the quotations we obtain and supply contracts we conclude in relation to our business and in providing our services to our clients. The legal basis on which the Company processes supplier information includes consent or concluding and performing contracts with suppliers or our legitimate interests in managing relationships and communicating with our suppliers, receiving, processing and paying supplier invoices, complying with applicable laws including tax laws, dealing with disputes and claims by and against us relating to any of our suppliers, including legal proceedings in any forum.

SHARING YOUR PERSONAL INFORMATION WITH OTHERS

The Company will not sell personal information to anyone.

When necessary, our trusted third party operators process personal information for us. The Company contracts with our operators binding them to comply with applicable data privacy laws including POPIA. Our contracts oblige our operators to process information only for the purposes and means of processing we prescribe.

The Company uses the following service providers to process personal information : hosting provider, web analysis service provider, providers of online platforms, IT programming and maintenance service providers (including website and email exchange), archiving and document storage service providers (electronic and hard copy), practice management system service providers, payroll service providers and data destruction service provider (physical files).

The Company discloses personal information to regulators and law enforcement agencies where required by law and where we reasonably believe disclosure is necessary to identify, contact or stop someone who may breach our privacy policy or who may cause harm to, or interfere with, our property, safety or interests or those of anyone else including other users of our website or our social media accounts.

The Company discloses personal information to underwriters and professional advisors when necessary so that we can obtain or maintain insurance cover, manage risk, get their advice or to establish, exercise or defend our rights including in relation to claims by or against us in any legal proceedings in any forum and in any negotiation.

The Company discloses Employee information to medical schemes, retirement funds, group life underwriters and brokers for these schemes and funds for the purposes of making benefits available to our partners, employees, their families and beneficiaries.

OFFSHORE TRANSFERS

Where the data subject publishes information on the Company website or on the Company's social media accounts or where the data subject instructs the Company to use an online platform which transfers personal information offshore, the data subject consents to the transfer of their personal information to third parties in foreign countries and they acknowledge that the personal information may be available through the internet around the world. The Company cannot prevent unauthorized access to, misuse of, damage to, or destruction of, that personal information.

If the Company is obliged by law to use an online platform which may transfer personal information offshore, we do not control that online platform and the Company cannot prevent unauthorized access to, misuse of, damage to, or destruction of, that personal information.

Where the Company transfers personal information to countries which do not have an adequate level of data protection similar to POPIA's conditions for lawful processing and the transfer is not covered by Section 72(1)(b)(consent to transfer),(c)(transfer needed to perform a contract with the data subject or to take pre-concept steps, (d) (transfer needed to conclude or perform a contract in the data subject's interests) or (e) (the transfer is for the data subject's benefit and it's not reasonably practicable to obtain the data subject's consent) of POPIA, the Company will conclude contracts with third parties to whom the information is transferred binding them to process the data subject information to the standards required by POPIA and not transfer your information to any other country without similar protection.

If a Microsoft Teams meeting with the Company is recorded, that recording may be stored on Microsoft OneDrive which is backed up in the European Union. The European Union has data protection laws which provide an adequate level of protection that upholds principles for reasonable processing of personal information substantially similar to the conditions for lawful processing applied by POPIA.

MANDATORY AND VOLUNTARY DISCLOSURE

Where the Company must collect and process personal information to comply with the law, we cannot provide services to the data subject unless he/she provides that information.

Except where providing personal information to the Company is required by law, our clients are free to volunteer personal information to us. If a client chooses not to provide personal information which we request to enable us to provide our services, this may restrict or prevent us from providing our services to that client.

PROTECTING PERSONNEL INFORMATION

The Company takes appropriate and reasonable technical and organisational steps to protect the data subject personal information against unauthorised access or disclosure.

The steps the Company takes includes physical and electronic access control, encryption, appropriate firewalls and malware and virus protection.

RIGHTS OF ACCESS, RECTIFICATION AND COMPLAINT

GDPR stipulates certain rights which should be made enforceable for data subjects. Data subjects have the right of access to 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

Subject to POPIA and other laws, by completing and sending us the request form available on request from Diana.Mcilrath@bellequipment.com, you may:

- ask to confirm, free of charge if the Company holds personal information about you,
- for the prescribed fee obtain a record or description of the personal information the Company holds and a list of third parties or the categories of third parties who hold it,
- where the legal basis on which the Company processes your personal information is consent, you may withdraw your consent but this will not affect the lawfulness of our processing before your withdrawal and even if you do withdraw your consent, the company can continue processing your information where there is another legal basis for that processing such as compliance with applicable laws,
- if any of your personal information that we have processed is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, obtained unlawfully or if we are no longer authorised to retain that personal information, you may ask us to rectify destroy or delete the personal information but we emphasize that despite your request, we may not destroy or delete personal information where we are entitled to continue processing it,
- at any time on reasonable grounds and except where legislation provides for such processing, object to the processing of your personal information for the proper performance of a public law duty by a public body or to pursue your legitimate interests or to pursue our legitimate interests or those of a third party to whom the personal information is supplied,
- at any time, object to the processing of personal information for direct marketing (other than direct marketing by means of unsolicited electronic communications),
- if you feel that we have processed your personal unlawfully, complain to the Information Regulator who can be contacted at:
    - JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
    - P.O. Box 31533, Braamfontein, Johannesburg, 2017, or
    - Complaints email: compliants.IR@justice.gov.za

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 Company's Data Protection Officer, via the contact details provided in Annex 4 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.

An updated version of the policy will be updated on the Company website. Important changes to the policy will be communicated via email to all employees. A current version of the policy can be obtained at any time by emailing a request to Diana.Mcilrath@bellequipment.com

ANNEX A: NOTIFICATION OF A SECURITY COMPROMISE FORM (SCN1)

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Note:

1. Attach documents in support of the notification
2. Complete the form in full as is applicable
3. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

A	DETAILS OF RESPONSIBLE PARTY
Name(s) and Surname/Registered name of responsible party:	
Address:	
	Code:
Contact Number(s):	
E-mail Address:	
B	**DETAILS OF THE INFORMATION OFFICER**
Full names of Information Officer:	
Registration number of information Officer:	
Contact Number(s):	
E-mail address:	
C	**DETAILS OF SECURITY COMPROMISE**
Date of incident:	
Date incident reported to Information Regulator:	
Explanation for delay in notification to the Regulator, if applicable.	
Kindly tick applicable box √	
Type of security compromise	Loss of personal information: Damage to personal information ☐ Unauthorised destruction of personal information ☐ Unlawful access to personal information ☐ Unlawful processing of personal information ☐ Other ☐ If other, please explain _____
Description of incident	

Kindly tick applicable box √	
Type of personal information compromised	Personal information of children ☐ Unique Identifiers ☐ Special Personal Information ☐ Other ☐
Number of data subjects affected	
Method of notification to affected data subjects	Mail to the data subject's last known physical or postal address, ☐ Sent by email to the data subject's last known email address, ☐ Placed in a prominent position on the website of the responsible party, ☐ Published in the news media ☐
Does the notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including--	A description of the possible consequence of the security compromise, ☐ A description of the measures that the responsible party intends to take or has taken to address the security compromise, ☐ A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise, ☐ If known, the identity of the unauthorised person who may have accessed or acquired the personal information. ☐
Status of the compromise	Confirmed: ☐ Alleged: ☐
D	**DESCRIPTION OF THE MEASURES THAT THE RESPONSIBLE PARTY INTENDS TO TAKE OR HAS TAKEN TO ADDRESS THE SECURITY COMPROMISE AND TO PROTECT THE PERSONAL INFORMATION OF THE DATA SUBJECTS FROM FURTHER UNAUTHORISED ACCESS OR USE.**
E	**DECLARATION**

I declare that the information contained herein is true, correct and accurate.

Signed at _____ on this the _____ day of _____20_____

_____
SIGNATURE

_____ _____
NAME AND SURNAME DESIGNATION

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. (Regulation 7)

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:	
Identity Number	
Physical Address;	
Postal Address:	
Telephone Number:	
Cellular Number:	

DETAILS OF THE REQUEST

Provide a detailed description of the information require:

CONFIRMATION OF IDENTITY OF DATA SUBJECT

_____, 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:	
Identity Number:	
Physical Address:	
Postal Address:	
Telephone Number:	
Cellular 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: FORM 1 – OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

ANNEXURE 2 – FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013, (ACT NO 4 OF 2013)

(REGULATION 2(1))

NOTE:

- Affidavits or other documentary evidence as applicable in support of the objection may be attached.
- If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
- Complete as is applicable.

A	**DETAILS OF DATA SUBJECT**
Name(s) and Surname of data subject	
Unique identifier / Identity Number	
Residential, Postal or Business Address	
	Code( )
Contact Number(s)	
Fax Number / Email address	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and Surname of responsible person (*if the registered responsible party is* a natural person):	
Residential, Postal or Business Address	
	Code( )
Contact Number(s)	
Fax Number / Email address	
Name of public or private body (*if the*	

responsible party is not a natural person):	
Business Address:	
	Code ( )
Contact Number(s)	
Fax Number	
Email Address	
C	**REASON FOR OBJECTION (Please provide detailed reasons for the objection)**

Signed at _____, this _____ day of _____ 20___ .

_____

Signature of Data Subject(applicant)

ANNEX 3: FORM 2 – REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD

ANNEXURE 3 – FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013, (ACT NO 4 OF 2013)

(REGULATION 3(2))

NOTE:

- Affidavits or other documentary evidence in support of the request must be attached.
- If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
- Complete as applicable.

Mark the appropriate box with an "X"

☐ Request for: Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF DATA SUBJECT
Name(s) and Surname of data subject	
Unique Identifier / Identity Number	
Residential, Postal or Business Address	
Contact Number(s)	
Fax Number / Email address	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and Surname of Responsible party (if the responsible party is a natural person):	
Residential, Postal or Business Address	
Contact Number(s)	
Fax Number / Email address	

Name of public or private body (if the responsible party is not a natural person)	
Business address:	
Contact number(s):	
Fax number / Email address	
C	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATE SUBJECT /*DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER CONTROL OF THE REPSONSIBLE PARTY **(Please provide detailed reasons for the request)**

** Delete whichever is not applicable*

Signed at _____, this _____ day of _____ 20___ .

_____

Signature of Data Subject

ANNEX 4: 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

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**

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**