McINTYRE VAN DER POST
LAW FIRM

PROTECTION OF PERSONAL INFORMATION ACT

McINTYRE VAN DER POST INC. INTERNAL PROCEDURE DOCUMENT

SUBJECT: FORMAT, APPROVAL, UPDATE AND DATA MANAGEMENT RELATING TO OBTAINING, PROCESSING AND THE PROTECTION OF CLIENT DATA AS PRESCRIBED IN THE PROTECTION OF PERSONAL INFORMATION ACT AND AUGMENTED BY THE COMPANY'S STATUS AS ATTORNEYS, THE LEGAL PRACTICE ACT, THE CODE OF CONDUCT FOR LEGAL PRACTITIONERS AND THE COMMON LAW.

RESPONSIBLE PERSON/COMMITTEE: CEO / MANAGEMENT COMMITTEE

RISK OWNER: INFORMATION OFFICER

TITLE: PROCEDURES FOR THE LAWFUL PROCESSING AND PROTECTION OF CLIENT INFORMATION

COMPILED BY eas-e Fica (Pty) Ltd

DATE 10 June 2021

ISSUE 1.0

CURRENT AMENDMENTS AND APPROVALS

FIRST APPROVAL BY THE BOARD

Approved by (title)	Name	Signature	Date
Board Chairman	J J Kachelhoffer		10 June 2021

DISTRIBUTION

Divisions/Departments	**Name**
Board/Management committee members	**Board members:** J J Kachelhoffer E S Els A D Venter P H Henning C A van Tonder G H Bradshaw M C V Gerdener A S C du Preez L van Zyl L D van Vuuren A S Gwangwa **Management committee members:** E S Els G H Bradshaw L van Zyl
Heads of professional departments and all professional staff	Court department : J J Kachelhoffer Commercial department : J J Kachelhoffer Estates department : A S C du Preez Deeds department : C A van Tonder Finance department : K Smith
Head: Human Resources	K Smith
Head: Finance	K Smith

VERSION CONTROL

Issue #	Author	Reason	Date
01	JC vd Walt	Inception	10 June 2021

OTHER DOCUMENTS TO BE READ IN CONJUCTION WITH THIS ONE

1 Human Resources and Disciplinary Code
2 Promotion of Access to Information policy and procedure
3 POPI Internal Policy, consent and disclosure
4 FICA RMCP

BACKGROUND

We obtain personal data from all our clients, suppliers and employees to a greater or lesser extent. This procedures manual is drafted so as to generalise procedures across the enterprise where possible; and where not, to provide for specific department-related procedures.

PROCEDURE 1: COLLECTION AND RETENTION OF QUALITY DATA FOR A SPECIFIC PURPOSE

The highest risk that we have to guard against here is that personal data is requested from clients where such data is not necessary for us to accept an instruction in a particular matter. We must ensure that we only obtain such information when it is strictly necessary to execute our mandate and the client has consented thereto in writing. It must be noted, however, that we are involved in the rendering of professional legal services where context plays an important role. In order to achieve an appropriate context it is often necessary to obtain information which may, at first glance, not appear to be strictly necessary. We therefore request our clients to provide us with as much relevant information as possible and rely on the professional discretion of our qualified staff to discern between more and less apposite information on a case-by-case basis bearing in mind the general principles of privilege applicable between attorney and client. Our general approach, however, is that all information we request and obtain is necessary for us to properly and effectively discharge our professional duties to our clients.

GENERAL PROCEDURE: PROFESSIONAL SERVICES	IS THERE AN ADDITIONAL DEPARTMENT-SPECIFIC PROCEDURE?	PERSON RESPONSIBLE
Only ask for personal information pertinent to the service to be rendered.	No, but see section on processing of data below.	Attorney and other professional staff
In respect of new clients, make necessary disclosure and obtain written consent for the collection of personal data as per disclosure document attached as Annexure 1, incorporated in our standard client mandate. In respect of existing clients, make separate disclosure and obtain written consent for the collection of personal data as per disclosure document attached as Annexure 1.		Attorney and other professional staff
Ensure that where you ask for information and the client declines, you respect that decision unless you cannot execute the mandate without the information and to proceed you are required to get information by law e.g. FICA.	Decline the instruction if the client refuses to provide you with sufficient information to execute the mandate or as required by law.	Attorney and other professional staff;
Ensure that you only deal with personal data obtained directly from the client or from someone within our own practice and/or a correspondent.	New information may come to light from time-to-time and from other sources, especially in the course of litigation. Ensure that all such information is acknowledged by the client in accordance with established good practice.	Attorney and other professional staff
GENERAL PROCEDURE: FINANCE DEPARTMENT – TO MAKE AND RECEIVE PAYMENTS	**IS THERE AN ADDITIONAL DEPARTMENT-SPECIFIC PROCEDURE?**	**PERSON RESPONSIBLE**
Only ask for and act on personal information pertinent to the payment and/or billing service to be rendered as populated on the accounting system software.	When requests for 3rd party payments are received, no payments can be made unless the 3rd party's identity has been established in terms of the FICA	HOD – K Smith

	RMCP and written consent as per Annexure 2 has been obtained. The same applies when a client's account is paid by a third party.	
GENERAL PROCEDURE: HUMAN RESOURCES DEPARTMENT	**IS THERE AN ADDITIONAL DEPARTMENT-SPECIFIC PROCEDURE?**	**PERSON RESPONSIBLE**
Only ask for personal information pertinent to employment as per Annexure 3.	No	HOD
In respect of existing employees, make separate disclosure and obtain written consent for the continued collection and processing of personal data as per disclosure document attached as Annexure 3.	No	HOD
GENERAL PROCEDURE: WEBSITE	**IS THERE AN ADDITIONAL DEPARTMENT-SPECIFIC PROCEDURE?**	**PERSON RESPONSIBLE**
Add disclosure form as per Annexure 4 to our website and ensure that all new visitors to our site must first consent to the terms and conditions and disclosure before access to navigate the site is enabled.	No	L D van Vuuren (Director)

CONTROL AND COMPLIANCE REQUIREMENT

The Information Officer (IO) must cause annually or more regularly if, in the exercise of his/her discretion e.g. when complaints are received, that all client records are audited to determine whether the requisite written disclosure and consent has been signed by the client. In the event that any complaints had been received in the course of any year or pertinent amendments were made to the Act, the IO must review the adequacy of the disclosure and consent form in the light of the nature of the complaints received and/or the amendments to the Act – as the case may be.

The IO must cause annually that all employee records are audited to determine whether the requisite written disclosure and consent has been signed. In the event that any complaints had been received in the course of any year or pertinent amendments were made to the Act, the IO must review the adequacy of the disclosure and consent form in

the light of the nature of the complaints received and/or the amendments to the Act – as the case may be.

The IO must cause annually that a review of the website terms and conditions are performed by reference to their continued adequacy and seek written confirmation from L D van Vuuren that the electronic signature function on the website remains functional.

The IO must, on an ongoing basis, respond to complaints individually but also by making recommendations regarding changes to our procedures and consent form content in order to mitigate the incidence of personal information-related complaints where such changes are deemed urgent and necessary by her/him.

PROCEDURE 2: THE LAWFUL PROCESSING OF PERSONAL INFORMATION

The highest risk identified here is that personal information obtained for one business purpose is passed on for use by another department. This is permissible where the work is interrelated e.g. between two departments e.g. commercial and litigation but poses a risk where unnecessary personal data is relayed to the finance department for a purpose not directly related to their work.

GENERAL PROCEDURE	DEPARTMENT-SPECIFIC PROCEDURE	PERSON RESPONSIBLE
Do not ask for information about other persons from 3rd parties – always try to ask the person him/herself.	No	All
Make sure that people know why you need the information – and be ready to justify your request.	No	All
If you are going to pass the information to someone else, make sure that the client knows this.	Professional Services: The new client mandate must contain specific reference to our interaction with correspondent attorneys and our authority to convey personal information to them. Human Resources: The disclosure and consent form must contain specific authority to obtain information from 3rd parties e.g. credit bureau and verification	All

	agencies.	
Make sure that there is a legitimate reason for any personal client information given to you by someone else and that both you and the provider of the information are authorised.	No Be aware of the purpose for which general information available about the client may be processed to establish a profile of the client relating to money laundering and/or terrorist financing. Such a profile may not be privileged in terms of legislation and may be requested by the client.	All

CONTROL AND COMPLIANCE REQUIREMENT

The requirements set out in Procedure 1 above apply here. In addition, the IO must, prior to us engaging in any direct marketing campaigns, assure her/himself that we have a written agreement in place with any external agencies in terms whereof we are guaranteed by such agencies that they only use lawfully obtained data and we are indemnified by them against the unlawful use of personal information. The IO must approve every direct marketing initiative by us in writing.

PROCEDURE 3: TRANSPARENCY OF ACTIVITIES

The biggest risk here is that clients do not know why we collect the personal data that we do. This may cause uncertainty, develop into conflict and may ultimately be perceived as poor client service.

GENERAL PROCEDURE	DEPARTMENT-SPECIFIC PROCEDURE	PERSON RESPONSIBLE
Ensure that you know and are able to explain to customers why you are asking them for specific information. In particular, where you are passing the information on to others within the Company, make a point of telling the client.	No	All
We have specific and detailed disclosure and consent documentation which is required to be accepted by each client, employee and website visitor.	No	All

PROCEDURE 4: PROTECTION OF DATA

Our biggest risk here lays in the fact that we use external software systems imposed on us by or service providers such as Microsoft and Google as well as any back-up agents we may use. To a large extent, access to personal data cannot be restricted by us, and neither can we accept responsibility for the accidental loss or destruction of the data. We have to constantly take steps to mitigate this risk.

GENERAL PROCEDURE	DEPARTMENT-SPECIFIC PROCEDURE	PERSON RESPONSIBLE
Ensure that we have SLAs in place with all external data service providers to accommodate restriction of access to data.	Yes – IT only.	IO and HOD IT
Ensure that we have reasonable indemnities and warranties in place in the event of a breach by an external service provider.	Yes – IT only.	IO and HOD IT
Ensure that there is adequate access control and security for electronic data e.g. passwords on computers and logging of electronic footprint on servers. Ensure that you close and lock your computer when not at your desk at al times.	All departments but also for IT specifically.	HOD IT
Ensure that your hard copy records are safely put away and protected when you are not at your desk.	No	All

CONTROL AND COMPLIANCE REQUIREMENT

IO must annually require the HOD IT to provide certification that adequate electronic safeguards are in place to ensure data protection, including disaster recovery and back-up.

IO must review all SLAs to ensure that adequate protection is afforded to the Company.

PROCEDURE 5: ACCESS TO, AMENDMENT AND DESTRUCTION OF INFORMATION

This aspect does not pose any particular risk to us due to our client-centric approach to business. Where specific information regarding a client is requested that may fall in the

ambit of the list below, we will only be doing so in pursuance of a specific mandate or other legal obligation.

GENERAL PROCEDURE	DEPARTMENT- SPECIFIC PROCEDURE	PERSON RESPONSIBLE
Ensure that we don't ask personal details regarding religious, sexual orientation, political conviction, race or ethnic origin, trade union membership or criminal record unless a law or the client instruction requires this.	No	HOD Finance, HOD HR, Attorneys
Ensure that you do not ask for or process any personal data of any children unless required to do so by law or in terms of a specific client instruction. Ensure that you only obtain data about children from parents and/or guardians.	No	Attorneys
Ensure that clients and employees are aware of the content of the consent form and their right to access their information.	No	HOD HR, Attorneys
Ensure that all requests for personal information by clients and employees are adhered to within ten days which we deem to be a reasonable time. We do not charge a fee for the dissemination of the information unless so directed by the IO on a case-by-case basis, but we do require a written request together with proof of identity of the person requesting the information. Ensure that all requests for personal information by website visitors are referred to our website administrator within a reasonable time. We may charge a fee for the dissemination of the information in the event that we have to pay an external party to assist us with obtaining the requested	1. All requests must be directed at the IO who must authorise the relevant HOD to release the information subject to the limitations imposed by the PAIA. 2. All information to be released must be approved in writing by the IO.	

information and we do require a written request together with proof of identity of the person requesting the information.		
Ensure that all requests for correction or deletion of personal information made by a client, website visitor or employee are adhered to as soon as reasonably possible but subject to data retention prescripts in law.	1. IO must approve all corrections and deletions in writing to the HOD of the department concerned. 2. Where personal data is corrected and we maintain a business relationship with the client, the IO must inform the FICA Reporting Officer in order to update the Customer Due Diligence records maintained by her/him.	IO, HODs, RO.
Ensure that all data is permanently destroyed as soon as practical after expiry of the last date on which we are required to maintain information by or under any law.	No	IO

CONTROL AND COMPLIANCE REQUIREMENT

IO must maintain a register of all requests including whether the requested information was provided or declined and if declined, the reason therefore. IO to annually check that all information requests from clients are maintained in the register.

IO must oversee, or obtain written confirmation from each HOD that personal information which is no longer required to be kept has been destroyed in accordance with the requirements.

End

ANNEXURE 1: **PROFESSIONAL SERVICES**

PROTECTION OF PERSONAL INFORMATION: DISCLOSURE AND CONSENT

At McIntyre Van Der Post Inc., we place professional client service first. Our range of professional services is wide, varies in scope and we depend on our professionally qualified staff to determine, on a case-by-case basis, the exact information they require in order to effectively discharge our obligations to represent you in the best manner possible. This may include information relating to you, your children and any other children in respect of whom you are appointed as guardian regarding:

(a) race, gender, sex, pregnancy, marital status, nationality, race, ethnic or social origin, colour, sexual orientation, trade union membership, political conviction, health or sex life, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;

(b) education or your medical, financial, criminal (including allegations levelled against you/them) or employment history;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to you/them;

(d) biometric information;

(e) personal opinions, views or preferences;

(f) correspondence sent by you /them that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about you; and

(h) your/their name if it appears with other personal information relating to you/them or if the disclosure of your/their name itself would reveal information about you/them.

Where we ask you about your personal information for legal advisory and assistance purposes, we act as your agent with your opponents and other counter-parties as well as correspondent attorneys, advocates and officers of court and must disclose your information to them. In matters of litigation and court proceedings, many aspects of your personal information as disclosed by us in law may become a

matter of public record. When we reach agreement in respect of the services we are instructed to render to you, we may also incur a legal obligation to share your data with the Financial Intelligence Centre or other supervisory bodies lawfully appointed by the Centre. It must be noted that in order to fully discharge our duties under the FIC act, we may be required from time-to-time, to process information about you obtained from various sources including credit bureaus, media and other publicly available sources in order to draw a risk profile of you. Lastly, we share such information about you as is necessary for billing and payment purposes, with our finance department and certain outsourced providers to them for purposes of debt recovery. In every instance where we obtain your personal information, we undertake that we:

- have a defined business purpose;
- retain your data only as long as we need it for business purposes or required by law;
- destroy your data comprehensively as soon as we may after expiry of our business purpose;
- will ask your consent if we are going to pass your data on to another entity or service provider not already mentioned herein, for instance for marketing or communication purposes;
- will not use the information to unlawfully infringe on your privacy in any way;
- will provide you with a complete record of all your personal data we hold and will update this at your request and will remove this, where we are permitted to by law, at your request;
- take measures to protect your personal data and where we use external parties such as software and internet service providers and we have agreements in place to reasonably protect your data.

You may at any stage, if you wish to lodge a complaint, contact our Information Officer at karin@mcintyre.co.za or telephone number 051 5050 200 and failing resolution, contact the Regulator. You may also and at any stage ask us to disclose the information we have about you and you may request us to update that information if it is no longer relevant or correct.

In the event of termination of our mandate and consequent to your instruction to us to provide any new service provider with all your detail, all our obligations in respect of your personal data shall cease once such transfer has occurred, save where we are required by law to retain such detail.

By your signature of our mandate of which this disclosure and consent forms a part, you agree that you have read, understand and consent to the content hereof.

ANNEXURE 2

POPIA DISCLOSURE AND CONSENT TO OBTAIN INFORMATION RELATING TO CUSTOMER DUE DILIGENCE IN TERMS OF THE FICA PURSUANT TO A REQUEST FOR 3RD PARTY OR VENDOR PAYMENT

DISCLOSURE AND CONSENT FOR CUSTOMER DUE DILIGENCE IN TERMS OF THE FINANCIAL INTELLIGENCE CENTRE ACT

McIntyre Van Der Post Inc. is an accountable institution as defined in the Financial Intelligence Centre Act. We have been requested to make payment to you on behalf of a client of ours. We are required by law to obtain and process information about you for the purposes of conducting Customer Due Diligence"(CDD) and which may include enhanced due diligence. The purpose of CDD is to determine the risk that you may be engaged in money-laundering and/or terror-financing activities. We are required to obtain and process information about you in respect of the following:

- Your identity and that of any person whom you purport to represent, including your status as a prominent person as defined in the act;
- Your place of residence and/or registration of your business;
- Your status as defined by reference to sections 26A (i.e. whether you are a person against whom financial sanctions have been imposed) and section 28A (i.e. whether you are a person in respect of whom there is an absolute prohibition against doing business with);
- The nature and ownership/control structure of your business; and
- The nature of our products and services, how they relate to your requirements and how you use them.

In certain circumstances and in the course of our CDD activities, we may avail ourselves of detail available about you in the public domain as well as additional detail we require to verify some of the information we collect about you. These sources may include commercially and publicly available information with regards to references made about and by you in, including but not limited to, the press and media including social media, law enforcement agencies such as Interpol and information collected and processed about you by credit bureaus and similar agencies including the verification of bank account details in your name.

You hereby consent to and authorize us and any agency lawfully appointed by us to obtain and process the information as described above as part of our duty in law.

ANNEXURE 3: **HUMAN RESOURCES**

PROTECTION OF PERSONAL INFORMATION: DISCLOSURE AND CONSENT

At McIntyre Van Der Post Inc., we place emphasis on our relationship with employees and prospective employees. We wish to appoint and retain employees best suited for their post and this requires a great deal of mutual transparency, disclosure and trust – demands to which gravity is added due to our position as attorneys and the ethical demands made on us by our clients. We must therefore be absolutely sure that us and you are a good fit and also for the following reasons: verification of an applicant's information during recruitment; general matters relating to employment including pension, for medical aid and health-related information administration, for our payroll administration, for training and disciplinary actions and any other matters required in the ordinary course of an employment relationship. We will therefore access and share your personal information with your prospective manager(s) upon you making application for a position with us and from time-to-time thereafter as required by good practice and our internal policies. In particular the information we will access may include information about:

(a) race, gender, sex, pregnancy, marital status, nationality, race, ethnic or social origin, colour, sexual orientation, trade union membership, political persuasion, health or sex life, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;

(b) education or your medical, financial, criminal (including allegations levelled against you/them) or employment history;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to you/them;

(d) biometric information;

(e) personal opinions, views or preferences;

(f) correspondence sent by you /them that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about you; and

(h) your/their name if it appears with other personal information relating to you/them or if the disclosure of your/their name itself would reveal information about you.

Where we ask you about your personal information we may submit same to external verification agencies such as credit bureaus and others. In every instance where we obtain your personal information, we undertake that we:

- have a defined and non-discriminatory business purpose;
- retain your data only as long as we need it for business purposes;
- destroy your data comprehensively as soon as we can after expiry of our business purpose;
- will ask your consent if we are going to pass your data on to an external agency not already referred to herein;
- will not use the information to unlawfully infringe on your privacy in any way;
- will provide you with a complete record of all your personal data we hold which we will update at your request and we will remove this, where we are permitted to by law, at your request;
- take measures to protect your personal data and where we use external parties such as software and internet service providers and we have agreements in place to reasonably protect your data.

You may at any stage, if you wish to lodge a complaint, contact our Information Officer at karin@mcintyre.co.za or 051 5050 200 and failing resolution, contact the Regulator. You may also and at any stage ask us to disclose the information we have about you and you may request us to update that information if it is no longer correct.

By your signature of our employment application documentation of which this disclosure and consent forms a part, you agree that you have read, understand and consent to the content.

Annexure 4

Website Privacy Policy for McIntyre Van Der Post Incorporated

Effective date: 10 June 2021

Version: 1.0

McIntyre Van Der Post Inc. ("us", "we", or "our") operate the www.mcintyre.co.za website and the content presented there (the "Service").

This page informs you of our policy regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data. This policy is part of, and must be read in the context of our overall policy regarding the protection of personal information as prescribed in the Protection of Personal Information Act. Where there are any inconsistencies between this document and our policy on the Protection of Personal Information, the wording of the latter shall prevail.

We use your data to provide and improve the Service. By using the Service i.e. by navigating on our website, you agree to the collection and use of information in accordance with this policy. Please be aware that different Services may also relate to their own set of specific terms and conditions.

Types of Data Collected

Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:

Identity details, Email address, Cookies and Usage Data

We may also collect information that your browser sends whenever you visit our Service or when you access the Service by or through a mobile device ("Usage Data"). This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access the Service by or through a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

Tracking & Cookies Data

We use cookies and similar tracking technologies to track the activity on our Service and to hold certain information.

Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies

also used are beacons, tags, and scripts to collect and track information and to improve and analyse our Service. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use:

Session Cookies. We use Session Cookies to operate our Service.

Preference Cookies. We use Preference Cookies to remember your preferences and various settings.

Security Cookies. We use Security Cookies for security purposes.

Use of Data

To provide and maintain the Service

To notify you about changes to our Service

To allow you to participate in interactive features of our Service when you choose to do so

To provide customer care and support

To provide analysis or valuable information so that we can improve the Service

To monitor the usage of the Service

To detect, prevent and address technical issues

Transfer of Data

Your information, including Personal Data, may be transferred to and maintained on computers located outside of your province, country or jurisdiction where the data protection laws may differ from those in your jurisdiction. If you are located outside South Africa and choose to provide information to us, please note that we transfer the data, including Personal Data, to our service providers in South Africa and process it there.

You consent to this Privacy Policy by your navigation of our website followed by your submission of such information and in the alternative, continued use of our Service represents your agreement to the transfer of information.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure of Data

Legal Requirements

We may disclose your Personal Data in good faith when we believe that such action is necessary:

To comply with a legal obligation

To protect and defend the rights or property of McIntyre Van Der Post Inc.

To prevent or investigate possible wrongdoing in connection with the Service

To protect the personal safety of users of the Service or the public

To protect against legal liability

Security of Data

The security of your data is important to us but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

Service Providers

We may employ third party companies and individuals to facilitate our Service ("Service Providers"), to provide the Service on our behalf, to perform Service-related services or to assist us in analysing how our Service is used. These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Links to Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Children's Privacy

Our Service does not address anyone under the age of 18 ("Children"). We do not knowingly collect personally identifiable information from anyone under the age of 18 unless required to do so by law and as part of an expressly stated mandate. If you are a parent or guardian and you are aware that your child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we will take steps to remove that information from our servers.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page under a sequential version number and effective date.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, please contact our Chief Information Officer by using the "Contact Us" facility provided on our website.

End V1.0