eNoteFile Data Processing Addendum

A summary of this Addendum:
This Data Processing Addendum helps demonstrate our organisation's priority regarding data protection, privacy and security compliance and forms part of our wider commitment to accountability. It helps simplify complex obligations we have to regulations and protocols like the Australian Privacy Act and European Union's General Data Protection Regulation (GDPR) and provides the basis for our staff training and specific compliance practices.

The purpose of this Addendum:
eNoteFile provides software globally, including to European Union (EU) organisations and residents. The EU has a specific set of regulations regarding protecting the data of its citizens called the 'GDPR'. While eNoteFile has always aimed for high level data protection, we have further addressed our specific GDPR compliance. The GDPR's requirements apply to EU residents' personal data and anyone involved with eNoteFile who processes that information. The GDPR has key principles and data subject rights which are addressed in this document, and it outlines eNoteFile's commitment to meeting and being accountable to these.

The definitions of Data Subject, Controller and Processor:

- Data Subject: The term 'data subject' refers to any living individual whose personal data is collected, held or processed by an organisation. Personal data is any data that can be used to identify an individual, such as a name, home address or credit card number.
- Data Controller: An individual or organisation (you can have joint controllers) that decides how, what, and why data is collected. A data controller determines the purpose and means of processing personal data. They may store it using another company's cloud servers. For example, a website that collects customer data is a controller.
- Data Processor: An individual or organisation that stores data on behalf of the controller(s) and processes the data upon request. An organisation or system can act as both a controller and a processor.
- In relation to your use of the eNoteFile application, you and your team will be the data controller and we will be the data processor. In relation to your use of our website, we will be the data controller.

This Data Processing Addendum specifies our obligations as a data processor, and sets out that we:

- Only process personal data requested by the controller, including transfers of personal data to non-EU countries or international organisations;
- Ensure that whoever authorises the personal data processes will keep all information confidential;
- Implement appropriate technical and organisational measures to ensure the personal data is secure, for example by using encryption and data masking;
- Must not delegate to sub-processors without the data controller's consent;
- Assist the controller in responding to requests from data subjects when they exercise their rights under the GDPR;
- Support the controller in ensuring compliance with its obligations in relation to data breach or data protection impact assessments;

- Delete or return all personal data to the controller when the controller so decides; and
- Will assist the controller's compliance with the GDPR, such as by helping with audits and inspections;
- Must inform the controller if one of the controller's instructions infringes the GDPR or any other data regulation.

Consent:
We request consent, declare our terms and state our privacy policy clearly and concisely, and gather consent each time it is needed. We also make it easy to withdraw consent. Valid consent for us needs to be freely given, specific to a purpose, and unambiguous. We inform data subjects about how we use their data.

Data breach:
We will notify all data subjects and relevant authorities that a security breach has occurred as soon as practical as part of our incident response policy. The notification includes information about what data was compromised, when it occurred, the status of the security vulnerability, and procedures on how data subjects can get more information.

Right to access:
At a data subjects request, we will provide confirmation as to whether personal data pertaining to them is being processed, where it is being processed, and for what purpose. We will also provide a copy of the personal data being processed in an electronic format.

Right to be forgotten:
We will erase all personal data when asked to do so by a data subject. At that point, we will stop any further dissemination or processing of the data. Valid conditions for erasure also include situations where the data is no longer relevant, or the original purpose has been satisfied.

Data portability:
We provide mechanisms for a data subject to receive any previously provided personal data in a commonly used format that can be transferred to another organisation.

Privacy by design:
We follow privacy by design principles and implement appropriate technical and organisational measures to protect the rights of data subjects. We only process the data necessary for the purpose of providing our service and limit access to personal data to only those employees needing the information to complete the process consented to by the data subject. We educate employees about the GDPR and use Data Protection Impact Assessments (DPIA) to help identify and minimise the data protection risks of a project.

Data protection officer:
We maintain thorough and comprehensive records pertaining to the collection, processing, and storage of personal data. In addition, we have a Data Protection Officer (DPO) to oversee the application of our privacy policy and to protect personal data from misuse and unauthorised access, and any other security breaches. We have policies dealing with confidentiality, intrusion detection, data classification, privacy protection, password management, auditing and logging, and encryption. We conduct regular evaluations of the data protection policies and procedures implemented by any

third-party contractors or partners to analyse any risks. To contact our Data Protection Officer please email: dpo@enotefile.com.

Third-party services we use and their GDPR compliance:

Clinical Notes application:
Dropbox: https://www.dropbox.com/security/GDPR
Microsoft Azure: https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR
Amazon Web Services: https://aws.amazon.com/compliance/gdpr-center/
TeamViewer: https://www.teamviewer.com/en/gdpr/

WebNotes and Practice Manager applications:
Microsoft Azure (SQL, App Insights):
https://www.microsoft.com/enus/TrustCenter/CloudServices/Azure/GDPR
Amazon Web Services: https://aws.amazon.com/compliance/gdpr-center/
Chargebee: https://www.chargebee.com/security/gdpr/
Twilio: https://www.twilio.com/gdpr
SendGrid: https://sendgrid.com/policies/tos/

Internal and general use:
Salesforce: https://www.salesforce.com/eu/campaign/gdpr/
Xero: https://www.xero.com/au/campaigns/xero-and-gdpr/
Slack: https://slack.com/gdpr
Atlassian products - Jira, Confluence, Trello: https://www.atlassian.com/trust/privacy/gdpr Office 365 (Outlook email): https://www.microsoft.com/en-us/trustcenter/privacy/gdpr/gdproverview
PayPal: https://www.paypal.com/us/webapps/mpp/gdpr-readiness-requirements
National Australia Bank: https://www.nab.com.au/common/privacy-policy/gdpr
Rebtel: https://www.rebtel.com/en/legal-information/
SurveyMonkey: https://www.surveymonkey.com/curiosity/surveymonkey-committed-to-gdprcompliance/
Typeform: https://www.typeform.com/help/gdpr-compliance/
Facebook: https://en-gb.facebook.com/business/gdpr
Twitter: https://gdpr.twitter.com/en.html
LinkedIn: https://privacy.linkedin.com/gdpr
Power BI: https://powerbi.microsoft.com/en-us/blog/power-bi-service-and-mobile-april-2018feature-summary/#GDPR-whitepaper

Website use:
Google Analytics: https://privacy.google.com/businesses/compliance/#!?modal_active=none
Intercom: https://www.intercom.com/help/pricing-privacy-and-terms/data-protection/howintercom-complies-with-gdpr
VentraIP: https://ventraip.com.au/terms-policies-agreements/
Zoom: https://support.zoom.us/hc/en-us/articles/360000126326-Official-Statement-EU-GDPRCompliance
Cloudflare: https://www.cloudflare.com/en-au/gdpr/introduction/

Overseas transfers:
eNoteFile stores data in servers in Australia and overseas. We take reasonable steps to ensure that the recipient does not breach the Australian Privacy Act (APP) and General Data Protection Regulation (GDPR) by only using providers with approved codes of conduct or certification in place, in countries that provide an adequate level of data protection and where standard data protection clauses or binding corporate rules apply.

Cookies:
We explain how we use cookies and why, and give users a simple and clear option to choose which ones they consent to.

EU Representative for eNoteFile Services:

Stuart Boyd
eurep@enotefile.com
Carrer Lluis Vives 72B
08810 Sant Pere De Ribes
Barcelona
Spain

eNoteFile's Data Processing Addendum agreement is an extension to our existing User Terms and Privacy Policy. Where the Addendum covers similar points, the User Terms and Privacy Policy are the default: https://enotefile.com/user-terms/ and https://enotefile.com/privacy/.

This Data Processing Addendum forms part of the agreement between:

Name: _____

Position: _____

Signature: _____

Date: _____

On behalf of the user/clinic/organisation: _____

And

Name: Bruce Cohen

Position: Director

Signature: 

On behalf of eNoteFile Services.