

**DATA PRIVACY POLICY**

**FOR**

**AKIRO & ASSOCIATES ADVOCATES**

---

Dated **1<sup>st</sup> September 2023**

---

CERTIFIED TO BE TRUE  
for VCF Organization

---

ADVOCATE

**Table of Contents**

- 1. Introduction..... 3
- 2. About The Firm..... 3
  - 2.1 Application of this Privacy Policy:..... 3
  - 2.2 Who We May Partner With: ..... 3
  - 2.3 How to contact us: ..... 4
- 3. Alliances and Adherence..... 4
- 4. The Firm User Types (including Opt Out Options)..... 4
  - 4.1 Site Visitors: ..... 4
    - 4.1.1 Type and Purpose of Collection**..... 4
    - 4.1.2 Site Visitor Data Sharing**..... 4
    - 4.1.3 Your rights** ..... 5
  - 4.2 Users:..... 5
    - 4.2.1 Type and Purpose of User Data Collection**..... 6
  - 4.3 Business Partners ..... 9
    - 4.3.1 Type and Purpose of Data Collected from Business Partners** ..... 9
    - 4.3.2 Business Partner Data Sharing** ..... 10
    - 4.3.3 Your rights** ..... 10
    - 4.3.4 Lawful Basis**..... 10
- 5. Data Security, Transfers, Sharing and Retention..... 10
  - 5.1 Security ..... 10
  - 5.2 Data Transfers Outside ..... 11
  - 5.3 Data Sharing..... 11
  - 5.4 Data Retention ..... 11
- 6. Children and Sensitive Data ..... 11
  - 6.1 Children..... 11
  - 6.2 Sensitive data..... 12
- 7. European Territory Visitors ..... 12
- 8. African Territories ..... 13
  - 8.1 Your privacy rights..... 13
  - 8.2 How to exercise your rights..... 13
- 9. “Do Not Track” Disclosure..... 14
- 10. Privacy Policy Amendments..... 14

**PRIVACY POLICY**

(For the Website/System)

---

**1. Introduction**

This privacy policy (hereinafter “**the Privacy Policy**”) governs the use of data collected by Akiro & Associates Advocates (hereinafter “**the Firm**”, “**us**”), including any and all personal data collected by us. Personal data is information that relates to you and may identify you as an individual whether natural person or legal person. We use your personal data in line with all applicable laws. To ensure compliance and to align with the Firm’s values around integrity, accountability, professionalism, trust and transparency we have a team of privacy professionals responsible for continuously implementing our cross-border privacy programs.

**2. About the Firm**

The Firm is a medium-size full service tech savvy law corporation that carries on the business of provision of legal services which include legal representation, legal consultancy, policy drafts and reviews, marketing of the law firm and its services, legal advisory services, authentication of legal documents i.e. commissioning and notarizing documents, publication of assorted articles and such other services as shall be from time to time designated by the Firm. The Firm further maintains various mobile and web applications and Firm Management Systems which helps it to carry out business and achieving its goal of a paperless law service provision to its vast clients. The Applications and Systems are from time to time maintained and made ready to subscribers, users and/or clients; to produce, process, prepare, control, extract, manipulate or otherwise experience our services and preparations of any nature of service or descriptions whatsoever.

**2.1 Application of this Privacy Policy:**

This Privacy Policy applies to The Firm and its affiliated subsidiaries (jointly and severally known as “Akiro & Associates”, “Akiro & Associates Advocates”, “the Firm”, “we”, “us”, “our”). We operate various offices across Kenya around partner with other Law Firms and/or Counsels across the world maintaining and serving various clients such as state corporations, various levels of governments, financial institutions, corporate entities, NGOs, Political outfits, Media Houses, Health Centres & Departments, Immigration & Foreign Institutions and other notable clients in many countries.

**2.2 Who We May Partner With:**

The Firm’s mission is to serve interesting recommendations to you based on what we believe are your interests. To achieve our mission, we enter into agreements with:

- a) Established Law Firms across the globe;
- b) Qualified & Practicing Advocates/Attorneys;
- c) Various Consultants including Legal & Financial Consultants;
- d) Registered Court Process Servers;
- e) Media Centres, Marketers & Advertisers;
- f) Financial Institutions such as Banks, Microfinance & Credit Facilities etc;
- g) Various levels of Governments;
- h) ICT & Software Engineers;
- i) Graphic Designers & Web Developers; and/or
- j) third party partners who help us serve you accordingly.

### 2.3 How to contact us:

We regularly review our compliance with this Privacy Policy. Questions, comments and requests regarding this Privacy Policy are welcome and should be addressed in the first instance to [privacy@akirolaw.com](mailto:privacy@akirolaw.com).

If The Firm does not satisfactorily answer your questions or concerns, you may also contact the following for advice, support or complaints:

- a) Our Data Protection Officer (“DPO”) at [dpo@akirolaw.com](mailto:dpo@akirolaw.com); and/or
- b) Your country’s Data Protection Authorities.

### 3. Alliances and Adherence

- a. We adhere to the Self-Regulatory Principles;
- b. We are duly registered as a Law Firm by the government of the Republic of Kenya (Registration Certificate No. **BN-L5CLVBKY**) and sanctioned, supervised or oversighted by the Law Society of Kenya (LSK); and
- c. We endeavor to partner with Firms and/or Law Practitioners who comply with their country’s licensing authorities.

### 4. The Firm User Types (including Opt Out Options)

Much of this Privacy Policy is divided into sections based on the way you may interact with the Firm. You are either a Site Visitor, a User and/or a Business Partner (as defined below). Please determine what user type you are. For each user type we’ve explained what information we collect and why, what cookies and other similar technologies we use, how we share such information and your rights.

#### 4.1 Site Visitors:

You are a Site Visitor when you visit and interact with our websites, web pages, interactive features, blogs and their respective contents at [akirolaw.com](http://akirolaw.com) (or any derivation, such as [akirolaw.ke](http://akirolaw.ke) etc.) (hereinafter “**Our Sites**”).

##### 4.1.1 Type and Purpose of Collection

We want to understand what services on Our Sites interest you and we want to remind you about these services we offer when you are not on Our Sites. In order to do this, we collect the following information from your device:

- (i) IP address;
- (ii) User Agent data: device type (e.g., iPhone), browser type (e.g., Chrome), operating system (e.g., iOS);
- (iii) the pages visited on Our Sites (e.g., the Firm “About” page);
- (iv) the time of visit (and corresponding time zone); and
- (v) referring URLs and other information normally transmitted in HTTP requests (e.g. information telling us how you arrived on Our Sites).

In addition, we may also collect your name and email address if you agree to send your details to us via Our Sites (e.g., by signing up to receive our newsletter).

##### 4.1.2 Site Visitor Data Sharing

We do not sell and/or share personal data about you with third parties for third party marketing or advertising purposes. We may use various third parties to help us market or advertise to you. We require that these third parties and companies agree to comply with all

applicable data protection laws, keep all information shared with them confidential and to use the information only to perform their obligations to us. We do this by entering into agreements with all third parties who process personal data. If you post on our blog, your comment and information will be publicly available. Please contact [support@akirolaw.com](mailto:support@akirolaw.com) to remove your comment from our Sites or database.

Our Sites contain links to other websites that we do not own or operate. We do not control, recommend or endorse the content, products, services, privacy policies or practices of these third party websites. For example, on Our Sites you will notice clickable icons which take you to the Firm's Facebook page or the Firm LinkedIn page. If you choose to click on these links, you should know that these sites are not owned or operated by the Firm and therefore these third party websites may send their own cookies to your device and they may independently collect personal data. It is therefore important that you get familiar with the privacy policies of these third party websites.

#### 4.1.3 Your rights

Our Terms of Use govern your use of Our Sites and apply to you when you interact with Our Sites. You can stop using Our Sites at any time. If you do, you may also want to remove any cookies that we have placed on any device used to access Our Sites, you can do this via your browser. If during your use of Our Sites you provided your email address, any email you receive from the Firm includes an "unsubscribe" option. In addition, you may also opt-out of direct marketing by emailing [support@akirolaw.com](mailto:support@akirolaw.com).

For Site Visitors in the European Territory, The Firm has implemented a consent management platform on Our Sites that provides you with the opportunity to consent, or not consent, to cookies and similar tracking technologies. Upon accessing Our Sites, you will see a banner in the page with information about the cookies we use. You may click the banner to reject any cookies (for example, performance cookies or targeting cookies) that are not strictly necessary cookies.

By pressing "**Accept**" on the banner you are indicating your acceptance to cookies and similar tracking technologies. The Firm's lawful basis for processing personal data of European Territory Site Visitors on Our Sites is consent. You may withdraw your consent at any time by not consenting or sending us an email at [privacy@akirolaw.com](mailto:privacy@akirolaw.com). In respect of all other Site Visitors not located in European Territories, we rely on our legitimate interest for processing any personal data. However, this does not preclude non-European Territory Site Visitors from withdrawing consent at any time via our consent management platform.

#### 4.2 Users:

You are a User when you visit a page of a website or application of one of the Firm's partners where the Firm's widget is installed or our recommendations are placed ("Partner Sites"). You know you are engaging with the Firm's widget when you see text referencing the Firm (e.g., "Recommended by Akiro & Associates", "by Akiro & Associates" near recommendations. If you click on the hyperlinked reference to the Firm you will see a detailed notice that enables you to navigate to the Firm's Portal and this Privacy Policy where you can opt out of personalized recommendations. In some instances, a partner may have white-label the Firm's service for their own offering. In such cases, such partners must disclose their use of the Firm in their privacy policies.

## 4.2.1 Type and Purpose of User Data Collection

We use Universally Unique Identifiers (UUIDs), IP Addresses and other Usage Information to enable us to serve interesting recommendations. The Firm's recommendations may be paid for by an advertiser linking you to a new website or they may be organic such that the link is to another page on the same Partner's Site.

The Firm may use high-level health interest categories to serve recommendations.

### 4.2.1.1 Universally Unique Identifiers

When you, as a User, first visit a Partner Site (such as facebook.com), The Firm drops a cookie on your device in order to generate a UUID. Alternatively, if you first interact with a Partner using that Partner's application, The Firm receives your advertiser ID which is assigned to you by your device. We catalogue and analyze the content you consume across Partner Sites. Our recommendations are based on:

- (i) a UUIDs browsing history;
- (ii) similar browsing patterns of other Users;
- (iii) recommendations that are generally popular with the Firm's audience at this time;
- (iv) some randomness, and
- (v) targeting requirements that may be provided or requested by our Amplify clients.

As an example, the Firm may know that, say UUID 123 (which could be you on your iPhone X on LinkedIn using Chrome as your browser) likes to read about Blockchain Regulations that people who like Digital Currency Laws also like Internet Money Transfers Legislations. When you interact with the Firm we do not collect traditional personal data from you, like your email address or name, therefore we cannot associate your name with your UUID.

The UUID is a sequence of numbers and/or letters which attaches itself to your device and varies depending on your browser combination. In other words, The Firm records a different UUID depending on which device and/or which browser you use when accessing the Partner Sites. For example, you will have one UUID when you visit a Partner Site from your mobile phone using Firefox, and a different UUID when you visit a Partner Site from your iPad using the browser Firefox. The Firm will combine and consolidate a UUID from a mobile device (handheld or tablet) from a browser that then accesses an application (or vice versa) from that same device. The Firm does not conduct cross device tracking and therefore cannot link a user interacting with the Firm on their phone as the same user who is interacting with the Firm on their desktop.

### 4.2.1.2 IP Address

In addition to your UUID, we recognize your IP address, which we translate into geolocation and delete some parts in order to mask the identifying information. We then use this masked information, in conjunction with information we received from other trusted third party partners (say lawQadverts.com) to determine a broad understanding of where you are located. The Firm will still recognize your IP address even if you opt out of personalised tracking as this is necessary to continue serving you context-based recommendations. However, in such instances, your IP address is not associated with your UUID and would not form part of any user profile.

### 4.2.1.3 Other Usage Information

We also collect the following information from you on:

**a) desktop and mobile web:**

- (i) User Agent data: device type (e.g., iPhone), browser type (e.g., chrome), operating system (e.g. iOS);
- (ii) the pages visited;
- (iii) the time of visit; and
- (iv) referring URLs and other information normally transmitted in HTTP requests.

The above statistical information provides us with information about how many Users visited a specific page on our Partner Sites on which the Firm's widget is installed, how long each User stayed on that page, the type of content on that page they clicked on and how they generally engaged with that page;

**b) on applications**

- (i) application version (as it appears in App Store or Play Store);
- (ii) application ID or package name (as it appears in the App Store or Play Store);
- (iii) operating system (e.g. IOS or Android);
- (iv) operating system version; and
- (v) device model (e.g. iPhone X).

This information is considered personal data if The Firm associates it with a UUID.

The Firm relies on its partners to determine the lawful basis upon which it can process personal data.

**c) Other similar data collection technologies we use**

**i. The Firm pixels**

Usually, some The Firm advertisers may implement the Firm pixel on their websites. The Firm pixel determines whether the User reaching the page where the pixel is installed has an The Firm UUID in order to provide reporting to advertisers in respect of their particular campaign. If there is a UUID associated with such end user, The Firm allows advertisers to either retarget those UUIDs and/or provides advertisers with the total number of Users (on an aggregated and anonymized basis) that reached a particular page (for example, an advertiser does not know that UUID1234 converted but only that one conversion took place).

The Firm does not pass its advertisers any personal data (including your UUID) or collect any further personal data via the pixel. The Firm does not combine information received from the Firm pixel information with a UUID's profile (for example, The Firm only tracks that one conversion has taken place and not the UUID123 has converted when it reaches the advertiser's chosen page).

We require advertisers to disclose the usage of the Firm pixel on their own websites. The Firm may also allow certain trusted third party partners to collect data via cookies delivered through the Firm widget. In such cases, The Firm does not pass these third parties the data which The Firm collects on its Users but allows such third parties to directly collect data (including personal data) via the widget for fraud and/or security purposes or in order to provide measurement information to advertisers (such as the number of conversions and/or impressions). Any such collection shall be governed by such third party's privacy policy.

## **ii. Third party pixels**

If you click on a link to one of our recommendations, the advertiser sponsoring the recommendation may place cookies (or third party cookies of third parties acting on the advertiser's behalf) on your device either through redirects prior to arriving on the destination page of the recommendations or upon reaching the destination page. Such cookies are dropped for the purposes of providing analytics to the advertiser with regards to the advertiser's campaign (for example, to see how many users viewed the advertiser's campaign).

We require our advertisers to disclose the use of third party pixels and/or cookies to end users via their website. As these cookies and/or pixels are added at the sole discretion of our advertisers you will be subject to that advertiser's privacy notice and/or privacy policy.

### **4.2.3 Data Sharing with our Partners**

The Firm does not share and/or sell a User's entire profiles with any third parties. However, we may share certain elements of a user profile (for example, UUID) with the following partners, including:

1. Brand and Data analytics partners;
2. Fraud Detecting partners;
3. Demand and Supply Side Platforms;
4. Ad Exchanges and/or Networks;
5. Demand Management Platforms;
6. Law enforcers on legal use/requirement basis

Additionally, we may collect and/or share some personal data with trusted partners by virtue of participating in the open industry standards of communication. For example, our Clients in Uganda's information will be shared with our partner advocates in Uganda for undertakings.

### **4.2.4 Your rights**

#### **4.2.4.1 The Firm opt out on desktop and mobile web**

You may opt out of the Firm's personalized recommendations (or, if you have opted out and would like to opt back in) at any time through provided means. You may also opt out of personalized recommendations via the Firm's general visualization of the data that the Firm knows about you and may use to make its recommendations in Our Sites.

#### **4.2.4.2 The Firm opt out on apps**

We will always provide an opt out means on our Apps to enable you to easily opt out. In case of queries, you are free to contact us.

Please note that an opt out via our Interest Profile and/or this Privacy Policy will not opt you out of personalized tracking on your applications. This opt out must be done via your device settings and/or browser.

#### **4.2.4.3 Additional Opt-Out Options**

You may also opt out of receiving personalized ads served by us or other advertising companies through industry powered tools. Unlike the Firm's opt out, these opt outs do not mean you



will no longer receive any advertising. The advertisements will just not be tailored to you. You will continue to receive advertisements, for example, based on the particular website that you are viewing (i.e., contextually based ads). Also, if your browsers are configured to reject cookies when you visit Our Sites, your opt out may not be effective as our opt out is cookie based.

#### 4.2.5 Important Information

Even though you have opted out of the Firm's personalized recommendations:

**You will still see the Firm recommendations.** Opting out of the Firm personalization tracking does not mean you will no longer receive recommendations from the Firm. Instead, it means that the Firm's recommendations will not be personalized (i.e. they will be context based recommendations).

**Your opt out will be cookie based and device/browser specific.** If you browse the web from several devices and/or browsers, you will need to opt out from each device and/or browser to ensure that we prevent personalization tracking on all of them. For the same reason, if you buy a new device, change browsers or delete (or clear) the opt out cookie, you will need to opt-out again. Opting out of personalization tracking is not the same as blocking cookies.

**You must not opt in to the Firm for at least 21 days as the deletion of your profile is tied to your UUID.** Your opt out from the Firm's personalized recommendations is effective immediately. However, if your browser permits local storage and you opt into the Firm's personalized recommendations (for example, by accepting a cookie banner) within 21 days of your opt out, it is possible your prior profile will be reconnected to your UUID. If you do not opt in within 21 days, your profile will be deleted and cannot be recovered.

**As with most opt out cookies, the Firm browser opt out relies upon a cookie.** The opt-out cookie is intended to be persistent to honor the user's preferences. However, the "Intelligent Tracking Prevention" feature in iOS may impact the persistence of cookies across websites. We suggest using another browser or considering blocking all 3<sup>rd</sup> party cookies from the browser so that you are "opted out" without needing to rely on any company's actual opt out methodology.

**Your local storage will not be cleared.** Even though you have opted out of the Firm's personalized recommendations, your local storage will not be automatically cleared and therefore you need to clear this at a browser level in addition to your opt out.

### 4.3 Business Partners

You are a Business Partner when you register (or email with the Firm) on behalf of the company you work for to use the Firm Services or you maintain an account with us.

#### 4.3.1 Type and Purpose of Data Collected from Business Partners

You may provide certain personal data (such as email address, telephone numbers, passwords, usernames, official names, financial transactions, legal issues or cases etc) when you sign up for the services or otherwise communicate or interact with us. If you apply to become a Business Partner, we may request additional information from you via advertiser application forms, insertion orders and other forms. We automatically collect information about your username's actions in the Firm's dashboard. As an example, as an Akiro & Associates Business Partner, if

you register an account as a client or advocate/lawyer, the Firm's dashboard trail will have a record of all those actions.

We collect and process the personal data above in order to perform our obligations under our agreement as a Business Partner (or prospective Business Partner) with you including to:

- respond to your questions and requests;
- to provide you with access to certain functions and features of our services (e.g., to provide and maintain your dashboard account);
- verify your identity; and
- communicate with you about your account, our services and available promotions relevant to your use of the service.

#### 4.3.2 Business Partner Data Sharing

We may disclose certain Business Partner information to vendors, contractors, or others who assist the Firm in delivering the services (e.g. Client names and Advocate names); refer further to the Sharing section of this Privacy Policy.

#### 4.3.3 Your rights

If as a Business Partner you wish to verify, correct, update or request the deactivation of your information, you may go to the Firm dashboard in order to edit your profile preferences or contact us at [support@akirolaw.com](mailto:support@akirolaw.com). If you are receiving the Firm emails, you may "unsubscribe" using a link in the email.

**TAKE NOTE** that unsubscribing shall not opt you out of notifications critical to providing the services (e.g., email invoices).

#### 4.3.4 Lawful Basis

The Firm's lawful basis for processing personal data of Business Partners is contractual.

### 5. Data Security, Transfers, Sharing and Retention

#### 5.1 Security

The Firm has a dedicated security team. We maintain tight controls over the personal data we collect, retaining it in firewalled and secured databases with strictly limited and controlled access rights, to ensure it is secure.

Business Partners have access to certain password-protected features of the system. Business Partners are responsible for keeping this password confidential and for ensuring the same for their employees and/or their agents. Please remember that, unfortunately, the transmission of information via the internet is never completely secure. A common Internet scam is known as "spoofing" or "phishing".

Spoofing or Phishing occurs when you receive an email from what appears to be a legitimate source requesting personal data from you. Please be aware that we will not send you any emails requesting you to verify credit card, bank information, or any other personal data. If you ever receive an email that appears to be from us requesting such information from you, do not

respond to it, and do not click on any links appearing in the email. Instead, please forward the email to us at [legal@akirolaw.com](mailto:legal@akirolaw.com), as we will investigate instances of possible Internet fraud.

## **5.2 Data Transfers Outside**

When we transfer personal data from Africa or Europe, we will ensure such transfers are in compliance with relevant data protection laws, including, if applicable, EU Standard Contractual Clauses, or a European Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC or Article 45 of the GDPR and such other African laws. In other words, your rights and protections remain with your data and we used approved contractual clauses and other measures designed to ensure that the recipients of your personal data protect it.

The Firm has in place the Standard Contractual Clauses between the Firm and entities to govern the transfer of data outside your locality.

## **5.3 Data Sharing**

We may share your personal data cautiously and in strict adherence to set laws and policies in the following, but not limited to, ways:

- Within the family of companies controlled by the Firm for internal reasons, primarily for business and operational purposes;
- If we go through a business transition, such as a merger, acquisition by another company, or sale of all or a portion of our assets, your personal data will likely be among the assets transferred;
- When legally required to do so (e.g., to cooperate with law enforcement investigations or other legal proceedings); and/or
- To respond to genuine emergencies.

Besides, we combine your personal data with those of other users in order to share trend information and aggregate user statistics with third parties, always in aggregated and anonymized form.

## **5.4 Data Retention**

The retention period for each of the cookies the Firm uses (whether our own or on our behalf by third parties) for about six (6) months. Nevertheless, some of the Firm cookies such as those used for tracking user actions such as clicks, expires three (3) months after a user visited a particular site within our network. However, these cookies will reset if a user returns to the same site or different site within our network. In addition, we do not retain any individual data point on a User for more than 13 months.

The Firm also maintains a Data Retention Policy that details the retention period for personal data based on our analysis of how long the specific data is reasonably required for legal or business purposes. When we no longer need personal data, we securely delete or destroy it. Aggregated data, which cannot identify a device/browser (or individual) and is used for purposes of reporting and analysis, is maintained for as long as commercially necessary.

## **6. Children and Sensitive Data**

### **6.1 Children**

None of our services are intentionally directed at children below the age of majority in every country of operation. We do not knowingly collect personal data from known children. If we determine upon collection that a Site Visitor, a User or a Business Partner is a child per law, we will not use or maintain his/her personal data. If we become aware that we have unknowingly collected personal data from a child, we will make reasonable efforts to delete such information from our records except for legal representation of which the consent shall be supplied by an adult user (i.e a next of kin or guardian).

If you're a kid, please go play in the yard, don't personally use or interact with the Firm!

## 6.2 Sensitive data

We may collect sensitive personal data relating financial activities etc. If we determine upon collection that a Site Visitor, a User or a Business Partner has provided sensitive data, we will bolster security of such sensitive personal data. If we become aware that we have unknowingly collected more than what is required, we will make reasonable efforts to delete such other information from our records.

## 7. European Territory Visitors

In compliance with certain privacy laws, in particular the Kenya Data Protection Act, 2019 and the European General Data Protection Regulation (GDPR), the Firm provides specific additional rights for individuals who interact with the Firm such as the right to access, rectification, right to object, to complaint, erasure and blockage. More specifically and under certain circumstances:

- a. the right to request information about whether and which personal data is processed by us, and the right to demand that personal data is rectified or amended.
- b. the right to request that personal data should be deleted.
- c. the right to demand that the processing of personal data should be restricted.
- d. withdraw your consent to the processing and use of your data completely or partially at anytime with future application.
- e. have the right to obtain your personal data in a common, structured and mechanically readable format.
- f. contact our data protection officer if there are any questions, comments, complaints or requests in connection with our statement on data protection and the processing of your personal data.
- g. the right to complain to the responsible supervisory authority if believed that the processing of your personal data is in violation of the legislation.

In addition to the above, we reference certain rights for European and Kenyan Territory citizens throughout this Privacy Policy. Pursuant to the GDPR, citizens from “**European Territories**” mean the European Economic Area (EEA), the European Free Trade Area (EFTA) and Switzerland. For the purpose of this Privacy Policy, the term “European Territories” shall continue to include the United Kingdom, even after the United Kingdom leaves the European Economic Area following Brexit.

If you are in the UK, or the European Economic Areas, the controller of your data is Akiro & Associates Advocates.

Please email [privacy@akirolaw.com](mailto:privacy@akirolaw.com) with any questions about exercising any of the above rights.

## 8. African Territories

This section applies only to African residents. It describes how we collect, use and share Personal Information of citizens of the African Countries in operating our business, and their rights with respect to that Personal Information.

### 8.1 Your privacy rights.

As an African resident, you have the rights listed below. However, these rights are not absolute, and in certain cases we may decline your request as permitted by the laws of your country.

- **Information.** You can request the following information about how we have collected and used your Personal Information during the past 12 months:
  - The categories of Personal Information that we have collected.
  - The categories of sources from which we collected Personal Information.
  - The business or commercial purpose for collecting and/or selling Personal Information.
  - The categories of third parties with whom we share Personal Information.
  - Whether we have disclosed your Personal Information for a business purpose, and if so, the categories of Personal Information received by each category of third party recipient.
  - Whether we've sold your Personal Information, and if so, the categories of Personal Information received by each category of third party recipient.
- **Access.** You can request a copy of the Personal Information that we have collected about you during the past 12 months.
- **Deletion.** You can ask us to delete the Personal Information that we have collected from you.
- **Opt-out of sales.** If we sell your Personal Information, you can opt-out. In addition, if you direct us not to sell your Personal Information, we will consider it a request pursuant to your country's laws to stop sharing your personal information covered by that country's laws with third parties for their direct marketing purposes.
- **Opt-in.** We contractually prohibit our publishing and advertising clients from placing our technology on pages that target individuals younger than 16 years old. If we learn that you are younger than 16 years old, we will be asking for your permission (or if you are younger than 13 years old, your parent or guardian's permission) to sell your Personal Information before we do so.
- **Non-discrimination.** You are entitled to exercise the rights described above free from discrimination. This means that we will not penalize you for exercising your rights by taking actions such as denying you services; increasing the price/rate of services; decreasing service quality; or suggesting that we may penalize you as described above for exercising your rights.

### 8.2 How to exercise your rights

You may exercise your privacy rights described above as follows:

- a) **Right to information, access and deletion.** You can request to exercise your information, access and deletion rights by:
- i) calling us on +254768229878 and accessing our contact us page to leave us a message.
  - ii) emailing [privacy@akirolaw.com](mailto:privacy@akirolaw.com)
  - iii) using the [web form](#) to submit your request(s) to us
- b) **Right to opt-out of the “sale” of your Personal Information.** We do not sell your Personal Information in the conventional sense (i.e., for money). However, like many companies, we use services that help deliver interest-based ads to you. Some Countries’ law may classify our use of these services as a “sale” of your Personal Information to the companies that provide the services. This is because we allow them to collect information from our website users (e.g., online identifiers and browsing activity) so they can help serve ads more likely to interest you. To opt-out from this “sale”, block ads from your browser.

We will need to confirm your identity and residency to process your requests to exercise your information, access or deletion rights. We cannot process your request if you do not provide us with sufficient detail to allow us to understand and respond to it.

## 9. “Do Not Track” Disclosure

Some browsers transmit Do Not Track (DNT) signals to websites. Because there is no common understanding of how to interpret the DNT signal, the Firm does not currently alter, change, or respond to DNT requests or signals from these browsers. We will continue to monitor industry activity in this area and reassess our DNT practices as necessary. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving personalized recommendations in the Users section.

## 10. Privacy Policy Amendments

We may change this Privacy Policy from time to time. We will place a prominent notice that will be visible to you as a Site Visitor or Business Partner, but we do not have a means of advising Users of an update by way of notice. You should check back here periodically to see if the Privacy Policy has been updated as we will always show the date of the latest modification of the Privacy Policy at the top of the page so you can tell when it was last revised.

---