



PwC Francophone Sub-Saharan Africa Data Protection Policy



Agenda

Introduction	7
Purpose and application	7
Data Protection by design	7
Data Protection by default	8
Lawful collection, processing, transfer and retention of personal data	8
Transparency – information to be given to data subjects	9
Security	9
Accuracy & integrity	9
Rights of data subjects	9
Record keeping	10
Breach notification	10
Data Protection Officer	10
Core scope of personal data processing activities in SSFA	11
Business contacts	11
Collection of personal data	11
Use of personal data	12
Administering, managing and developing our businesses and services	12
Carrying out market research and market analytics	12
Providing information about us and our range of services	13
Data Retention	13
When and how we share personal data and locations of processing	14
Corporate clients (and individuals associated with our corporate clients)	14
Collection of personal data	14
Use of personal data	15
Providing professional services	15
Legal grounds: Legitimate interests, legal obligation, public interest or consent	15
Administering, managing and developing our businesses and services	15
Legal grounds: Legitimate interests	15
Security, quality and risk management activities	16
Legal grounds: Legitimate interests	16
Providing our clients and prospective clients with information about us and our range of services	16
Legal grounds: Legitimate interests	16



Complying with any requirement of law, regulation or a professional body of which we are a member	17
Legal grounds: Legal obligation or legitimate interests	17
Legal grounds: Legal obligation or legitimate interests	17
Data Retention	17
When and how we share personal data and locations processing	18
Personal clients	18
Collection of personal data	18
Use of personal data	18
Providing professional services	19
Legal grounds: Performance of a contract, legitimate interests, legal obligation, public interest or consent	19
Administering, managing and developing our businesses and services	19
Legal grounds: Legitimate interests	19
Security, quality and risk management activities	20
Legal grounds: Legitimate interests	20
Providing our clients and prospective clients with information about us and our range of services	20
Legal grounds: Legitimate interests	20
Complying with any requirement of law, regulation or a professional body of which we are a member	21
Legal grounds: Legal obligation or legitimate interests	21
Legal grounds: Legitimate interests	21
Data retention	21
When and how we share personal data and locations of processing	22
Individuals who use our applications	22
Individuals whose personal data we obtain in connection with providing professional services to our clients	22
Collection of personal data	22
Use of personal data	23
Providing professional services	23
Legal grounds: Legitimate interests, legal obligation, public interest or consent	23
Administering, managing and developing our businesses and services	24
Legal grounds: Legitimate interests	24
Security, quality and risk management activities	24
Legal grounds: Legitimate interests	24



Complying with any requirement of law, regulation or a professional body of which we are a member	25
Legal grounds: Legal obligation or legitimate interests	25
Legal grounds: Legitimate interests	25
Others who get in touch with us	26
Personnel (partners, staff and contractors)	26
Recruitment applicants	26
Introduction	26
Collection of personal data	27
Use of personal data	27
Automated processing of personal data	29
Making an online application:	29
Online Assessments (Situational judgement tests and Game-based psychometric assessments):	29
Video interview:	29
When and how we share personal data and locations of processing	30
Other PwC member firms	30
Third party organizations that provide applications/functionality, data processing or IT services to us, or that provide screening services to us	30
Data retention	31
Suppliers (including subcontractors and individuals associated with our suppliers and subcontractors)	31
Collection of personal data	31
Use of personal data	31
Receiving services	32
Legal grounds: Legitimate interests	32
Providing professional services to clients	32
Legal grounds: Legitimate interests	32
Administering, managing and developing our businesses and services	32
Legal grounds: Legitimate interests	33
Security, quality and risk management activities	33
Legal grounds: Legitimate interests	33
Providing information about us and our range of services	33
Legal grounds: Legitimate interests	33
Complying with any requirement of law, regulation or a professional body of which we are a member	34



Legal grounds: Legal obligation or legitimate interests	34
Data retention	34
Visitors to our offices	35
CCTV	35
Visitor records	35
Guest WIFI	35
Visitors to our website	36
Collection of personal data	36
Use of personal data	36
Third party links	37
Data retention	37
Events	37
Introduction	38
Security	38
Changes to this privacy statement	38
Data controller and contact information	39
Collection of personal data	39
Use of personal data	39
When and how we share personal data and locations of processing	40
Third party organizations that provide applications/functionality, data processing or IT services to us.	40
Data retention	40
Individuals' rights and how to exercise them	41
Right of access	41
Right to rectification	41
The right to erasure / right to be forgotten	42
The right to restrict processing	42
The right to object to processing	43
Right to data portability	43
Right to withdraw consent	43
Complaints	43
Security	43
When and how we share personal data and locations of processing	45
Other PwC member firms	45
Third party organizations that provide applications/functionality, data processing or IT services to us	46



Third party organizations that otherwise assist us in providing goods, services or information	47
Our clients	47
Auditors, insurers and professional advisers	47
Law enforcement or other government and regulatory agencies or to other third parties as required by, and in accordance with, applicable law or regulation	48
Changes to this privacy statement	48
Data controller and contact information	48
Individuals' rights and how to exercise them	49
Your right of access to personal data	49
Your right to rectification / amendment of personal data	49
Your right to erasure / right to be forgotten	50
Your right to restrict processing	50
Your right to object to processing	51
Your right to data portability	51
Your right to withdraw consent	51
Complaints	52
ANNEXURES:	53
Annex-1 How we are structured	53
Annex - 2 - List of countries within PwC Sub Saharan Africa	55



1 Introduction

1.1 Purpose and application

As a member of the PwC network, PwC Sub-Saharan Francophone Africa (SSFA) must apply the requirements of the PwC network data protection policy through its own local policies. PwC SSFA must also ensure its local policies reflect the requirements of applicable privacy law within its territories, including GDPR obligations where applicable.

PwC SSFA is strongly committed to protecting personal data. This data protection statement describes why and how we collect and use personal data and provides information about individuals' rights. It applies to personal data provided to us, both by individuals themselves or by others. We may use personal data provided to us for any of the purposes described in this privacy statement or as otherwise stated at the point of collection.

“PwC” (and “we”, “us”, or “our”) refers to PricewaterhouseCoopers entities in the Sub-Saharan Francophone Africa region (Cameroon, Chad, Congo, Côte D'Ivoire, Democratic Republic of Congo (DRC), Equatorial Guinea, Gabon, Guinea, Mauritania, Madagascar, Senegal) and their subsidiaries that: (1) is a contracting party for the purposes of providing or receiving services, (2) posted a position for which you are applying, or (3) you have a role or relationship with. Each member firm in the PwC network is a separate legal entity and a separate controller for personal data.

Personal data is any information relating to an identified or identifiable living person. When “you” or “your” are used in this statement, we are referring to the relevant individual who is the subject of the personal data. PwC processes personal data for numerous purposes, and the means of collection, lawful basis of processing, use, disclosure, and retention periods for each purpose may differ.

When collecting and using personal data, our policy is to be transparent about why and how we process personal data. Minimum data protection requirements when processing personal data

PwC SSFA must comply with the minimum requirements in this section when processing or procuring processing of personal data.

1.2 Data Protection by design

When deciding how to process personal data and when processing it, PwC SSFA must implement technical and organisational measures (e.g. pseudonymisation) designed to implement data-protection principles (e.g. data minimisation) effectively and to integrate necessary safeguards into the processing in order to meet the requirements of applicable



privacy law. The measures must be appropriate considering (i) the state of the art (ii) the cost of implementation (iii) the nature, scope, context and purposes of the processing and (iv) the risk posed to data subjects.

1.3 Data Protection by default

PwC SSFA must put in place appropriate technical and organisational measures for ensuring that, by default, personal data is not processed unnecessarily. This applies to the amount of personal data collected, the extent to which it is processed, how long it is stored and who can access it. In particular, PwC SSFA must ensure that, by default, personal data is not made available to an indefinite number of people without some action by the data subject.

1.4 Lawful collection, processing, transfer and retention of personal data

PwC SSFA must:

- **[collection]** collect personal data only for identified and lawful purposes connected with the business of one or more PwC firms.
- **[processing]** process personal data only where it has a lawful basis for doing so under an applicable privacy law and in a manner that's lawful, fair and compatible with the purpose for which the personal data was collected
- **[data minimisation]** collect and process personal data that is adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data is processed
- **[retention]** retain personal data only:
 - to the extent and for so long as necessary in connection with the purpose for which PwC SSFA processes the personal data
 - as required by professional standards or Policies
 - as required or permitted by law.

PwC SSFA must delete, destroy or permanently anonymise all other personal data it processes.

- **[transfer]** transfer personal data only in accordance with applicable privacy laws.



1.5 Transparency – information to be given to data subjects

PwC SSFA must give data subjects information about its processing of their personal data in accordance with applicable privacy law and as required by paragraphs M, N and O of PwC Network Standard 10.6 on information protection. PwC SSFA must provide the relevant information within the timeframes specified in the relevant law.

1.6 Security

PwC SSFA must implement technical and organizational measures at least consistent with the PwC Network Information Security Policy and Standards to protect personal data against unauthorized or unlawful processing (including unauthorized disclosure, access, loss, alteration, damage and destruction). The measures must be appropriate considering (i) the state of the art (ii) the cost of implementation (iii) the nature, scope, context and purposes of the processing and (iv) the risk posed to data subjects.

PwC SSFA must restrict access to personal data to personnel with a need to know who are bound to maintain the confidentiality and security of the personal data and process it only on PwC SSFA's instructions or to comply with a Requirement of Law.

1.7 Accuracy & integrity

PwC SSFA must take commercially reasonable steps to update, correct, complete or delete (as appropriate) any personal data shown to be out of date, inaccurate or incomplete, to the extent required by applicable privacy laws.

1.8 Rights of data subjects

Where a data subject exercises a right under applicable privacy law, PwC SSFA must respond by taking any action required by the relevant privacy law, unless the request is obviously unfounded or excessive. PwC SSFA must take the relevant action within one month of receipt, unless a different time period is set by applicable privacy law.



1.9 Record keeping

PwC SSFA must:

- (a) include any local law record keeping requirements – or provide one set of requirements that meets local law and requirements when processing EEA personal data from paragraph (b)
- (b) when processing EEA personal data, maintain records of its processing operations that document the following:
 - its name and contact details
 - where applicable, the name and contact details of the PwC SSFA's data protection officer any joint controller
 - the purposes for which the relevant personal data is being processed
 - the categories of data subjects whose personal data is being processed and the categories of personal data being process
 - the categories of recipients to whom the personal data has or will be disclosed
 - transfers of personal data to non-EEA countries (naming the relevant non-EEA country)
 - where possible, the time limits for retaining different categories of personal data
 - where possible, a general description of the technical and organisational security measures minimally required as per this policy
- (c) make the record available to a relevant supervisory authority to the extent required by applicable privacy law.

1.10 Breach notification

PwC SSFA must comply with any applicable privacy law requirement to notify data subjects or supervisory authorities of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or, or access to personal data. PwC SSFA must also notify the breach to the Network Data Protection Leader in accordance with reporting guidelines approved by the Network Data Protection Governance Board for this purpose.

1.11 Data Protection Officer

PwC SSFA has designated its Technology Leader as SSFA Data Protection Officer. The DPO is supported by a NDDP Governance committee, which meets quarterly and ad-hoc if necessary



1.12 Core scope of personal data processing activities in SSFA

When collecting and using personal data, our policy is to be transparent about why and how we process personal data.

We have identified core areas within specific processing activities, which are subject to data protection obligations. Please go to the relevant sections of this statement as listed below.

- [Business contact](#)
- [Corporate clients \(and individuals associated with our corporate clients\)](#)
- [Personal clients](#)
- [Individuals who use our applications](#)
- [Individuals whose personal data we obtain in connection with providing professional services to our clients](#)
- [Others who get in touch with us](#)
- [Personnel \(partners, staff and contractors\)](#)
- [Recruitment applicants](#)
- [Suppliers \(including subcontractors and individuals associated with our suppliers and subcontractors\)](#)
- [Visitors to our offices](#)
- [Visitors to our websites](#)
- [Insolvencies and restructuring](#)
- [Events](#)

2 Business contacts

2.1 Collection of personal data

PwC processes personal data about business contacts including any of the following: existing and potential PwC clients, individuals associated with them, members of the press, legal and business advisers, and other third parties and intermediaries PwC interacts with in the course of business.

PwC may collect business contacts' details directly or indirectly from the business contacts, and/or from publicly available sources including social media sites, and/or from third parties, such as companies operating public relations or business development databases. PwC may collect details including name, contact details and other information (such as job title, employer, areas of business interest and other business details).



PwC processes personal data about business contacts using a customer relationship management system in use in SSFA (the “PwC CRM”).

In addition to the above, the PwC CRM may collect data from PwC email and calendar systems (names, date, and time) concerning interactions between PwC users and contacts or third parties.

2.2 Use of personal data

Personal data relating to business contacts may be used for our legitimate interests and the legitimate interests of other PwC member firms for any combination of the following purposes:

2.2.1 Administering, managing and developing our businesses and services

We may process personal data in order to run our business, including:

- managing our relationship with clients;
- developing our businesses and services (such as identifying client needs and improvements in service delivery and learning more about a client, relationship opportunity we or other PwC member firms have an interest in);
- analysing and evaluating the strength of interactions between a business contact and us. The PwC CRM uses an algorithm to help with this analysis and the ranking is primarily based on interaction frequency, duration, recency and response time;
- performing analytics, including (i) to produce metrics for PwC leadership, such as on trends, relationship maps, sales intelligence and progress against account business goals and (ii) in combination with various other client and sales related data, including past outcomes to identify actionable variables to assist our sales teams;
- maintaining and using IT systems;
- hosting or facilitating the hosting of events; and
- administering and managing our website, systems and applications.

2.2.2 Carrying out market research and market analytics

We may use business contacts’ information to conduct surveys or other forms of market research, and to carry out market analytics and profiling, so we can develop and offer appropriate products and services.



2.2.3 Providing information about us and our range of services

Unless we have been asked not to, we may collect, store and use business contact details to provide information to business contacts that we think will be of interest about our services and us. For example, press releases, industry updates and insights, marketing relating to other services that may be relevant and invitations to events. We may send you these communications by email, post, telephone and messages to your mobile phone and through social media. We will only send electronic marketing communications to business contacts in a business-to-business context, where we have the recipient's prior consent or where it is otherwise lawful to do so.

If you decide that you do not want to receive marketing communications from us, you can unsubscribe via the following channels: AFSS_mktcomms_unsubscribe@pwc.com

In that case, we will include your details on a suppression list, so we do not send you further marketing communications. We may still send you emails regarding factual, transactional and/or servicing information in connection with products or services we are providing to you or your organization.

PwC member firms do not sell or otherwise release personal data contained in the PwC CRM to third parties for the purpose of allowing them to market their products and services without consent from individuals to do so.

2.3 Data Retention

Personal data of clients, potential clients, or their associates will be retained on the PwC CRM or any other system used to manage clients projects for as long as we have, or need to keep a record of, a relationship with a business contact, which is for the duration of our relationship with a contact or their organization. Personal data of business contacts will be retained in line with our retention policy.

Personal data may be held for longer periods where extended retention periods are required by law or regulation and in order to establish, exercise or defend our legal rights.



2.4 When and how we share personal data and locations of processing

The PwC CRM is provided by Salesforce and is hosted in Salesforce's European data centers. Use of the PwC CRM is supported by additional functionality provided by Introhive including profiling, and certain personal data in the PwC CRM may be processed by Introhive on its servers. The information in the PwC CRM may be accessed by PwC member firms for the purposes described above. For details of our member firm locations, please [click here](#) or check the annexures. Further details about the processors (such as IT service providers) used by PwC and locations of processing are [provided here](#).

3 Corporate clients (and individuals associated with our corporate clients)

3.1 Collection of personal data

Our policy is to collect only the personal data necessary for agreed purposes and we ask our clients to only share personal data with us where it is strictly needed for those purposes.

Where we need to process personal data to provide professional services, we ask our clients to provide the necessary information to the data subjects regarding its use. Our clients may use relevant sections of this privacy statement or refer data subjects to this privacy statement if they consider it appropriate to do so.

The categories of personal data processed by us in relation to the services we provide are generally:

- Personal details (e.g. name, age/date of birth, gender, marital status, country of residence);
- Contact details (e.g. email address, contact number, postal address);
- Financial details (e.g. salary and other income and investments, benefits, tax status); and
- Job details (e.g. role, grade, experience and performance information).
- For certain services or activities, we may process special categories of personal data (such as in performing know your client checks and providing immigration and tax services, which involve us processing government identification documents that may contain biometric data or data revealing racial or ethnic origin or as part of an audit of an organization in the health sector).



- Generally, we collect personal data from our clients or from third parties when providing services to the relevant client.

3.2 Use of personal data

We use personal data for the following purposes:

3.2.1 Providing professional services

We provide a diverse range of professional services. Some of our services require us to process personal data in order to provide advice and deliverables. For example, we will review payroll data as part of an audit and we often need to use personal data to provide global mobility, tax and pensions services.

- **Legal grounds:** [Legitimate interests, legal obligation, public interest or consent](#)

This processing of personal data by us is necessary for the purposes of the legitimate interests pursued by us in providing professional services and our client in receiving professional services as part of running their organization and, in some cases, we have a legal obligation to provide the services in a certain way (e.g. statutory audit). Where we process special categories of personal data, we rely on a relevant public interest condition or consent.

3.2.2 Administering, managing and developing our businesses and services

We may process personal data in order to run our business, including:

- managing our relationship with clients and prospective clients;
- developing our businesses and services (such as identifying client needs and improvements in service delivery);
- maintaining and using IT systems;
- hosting or facilitating the hosting of events; and
- administering and managing our website, systems and applications.

- **Legal grounds:** [Legitimate interests](#)

This processing is necessary for the purposes of the legitimate interests pursued by us to administer, manage and develop our business and services.



3.2.3 Security, quality and risk management activities

We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for example, automated scans to identify harmful emails. We monitor the services provided to clients for quality purposes, which may involve processing personal data stored on the relevant client file. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to client engagements. We collect and hold personal data as part of our client engagement and acceptance procedures. As part of those procedures we carry out searches using publicly available sources (such as internet searches and sanctions lists) to identify politically exposed persons and heightened risk individuals and organizations and check that there are no issues that would prevent us from working with a particular client (such as sanctions, criminal convictions (including in respect of company directors), conduct or other reputational issues).

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to ensure network and information security, manage risks to our business and check the quality of our services.

3.2.4 Providing our clients and prospective clients with information about us and our range of services

Unless we are asked not to, we use client and prospective client business contact details to provide information that we think will be of interest about our services and us. For example, industry updates and insights, other services that may be relevant and invites to events.

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to promote our business and services.

3.2.5 Complying with any requirement of law, regulation or a professional body of which we are a member

As with any provider of professional services, we are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our



services are provided in compliance with those obligations and those records may contain personal data.

- **Legal grounds: [Legal obligation or legitimate interests](#)**

This processing is necessary for us to comply with a legal obligation; for example, when conducting customer due diligence checks to comply with anti-money laundering regulations and, where we do not have a legal obligation, we have a legitimate interest in processing personal data as necessary to meet our regulatory or professional obligations.

We are continually looking for ways to help our clients and improve our business and services. Where agreed with our clients, we may use information that we receive in the course of providing professional services for other lawful purposes, including analysis to better understand a particular issue, industry or sector, provide insights back to our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings. To the extent that the information we receive in the course of providing professional services contains personal data, we will de-identify the data prior to using the information for these purposes.

- **Legal grounds: [Legal obligation or legitimate interests](#)**

We have a legitimate interest in de-identifying data to help our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings, including by performing benchmarking and analysis.

3.3 Data Retention

We retain the personal data processed by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulation).

In the absence of specific legal, regulatory or contractual requirements, our baseline retention period for records and other documentary evidence created in the provision of services is 7 years.

Personal data may be held for longer periods where extended retention periods are required by law or regulation and in order to establish, exercise or defend our legal rights.



3.4 When and how we share personal data and locations processing

Further details about the processors (such as IT service providers) used by PwC and locations of processing are on request or in Annexures. We may use other organisations to help us deliver our services as agreed with our client on an engagement-specific basis.

4 Personal clients

4.1 Collection of personal data

Our policy is to collect only the personal data necessary for agreed purposes and we ask our clients only to share personal data where it is strictly needed for those purposes.

Where we need to process personal data to provide our services, we ask our clients to provide the necessary information to other data subjects concerned, such as family members, regarding its use.

Given the diversity of the services we provide to personal clients, we process many categories of personal data, including as appropriate for the services we are providing:

- Contact details;
- Business activities;
- Family information;
- Income, taxation and other financial-related details; and
- Investments and other financial interests.

For certain services or activities, and when permitted by law (e.g. under a public interest condition) or with an individual's consent, we may also collect special categories of personal data. Examples of special categories include *race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health; genetic data; biometric data; sexual life or sexual orientation; and, criminal records.*

Generally, we collect personal data from our clients or from a third party acting on the instructions of the relevant client.

4.2 Use of personal data

We use personal data for the following purposes:



4.2.1 Providing professional services

We provide a diverse range of professional services. Some of our services require us to process personal data in order to provide advice and deliverables. For example, we need to use personal data to provide individual tax advice, or payroll services.

- **Legal grounds: Performance of a contract, legitimate interests, legal obligation, public interest or consent**

This processing is necessary for the performance of the engagement letter (contract) to which our personal client (the data subject) is a party and, where we process personal data about other individuals (such as family members) in order to provide our services, this processing is necessary for the purposes of the legitimate interests pursued by us in providing professional services and our client in receiving professional services. In some cases, we have a legal obligation to provide the services in a certain way and where we process special categories of personal data, we rely on a relevant public interest condition or consent.

4.2.2 Administering, managing and developing our businesses and services

We may process personal data in order to run our business, including:

- managing our relationship with clients and prospective clients;
- developing our businesses and services (such as identifying client needs and improvements in service delivery);
- maintaining and using IT systems;
- hosting or facilitating the hosting of events; and
- administering and managing our website, systems and applications.

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to administer, manage and develop our business and services.



4.2.3 Security, quality and risk management activities

We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for example, automated scans to identify harmful emails. We monitor the services provided to clients for quality purposes, which may involve processing personal data stored on the relevant client file.

We have policies and procedures in place to monitor the quality of our services and manage risks in relation to client engagements. We collect and hold personal data as part of our client engagement and acceptance procedures. As part of our client and engagement acceptance, we carry out searches using publicly available sources (such as internet searches and sanctions lists) to identify politically exposed persons and heightened risk individuals and organisations and check that there are no issues that would prevent us from working with a particular client (such as sanctions, criminal convictions (including in respect of company directors), conduct or other reputational issues).

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to ensure network and information security, manage risks to our business and check the quality of our services.

4.2.4 Providing our clients and prospective clients with information about us and our range of services

With consent or otherwise in accordance with applicable law, we use client and prospective client contact details to provide information that we think will be of interest about us and our services. For example, industry updates and insights, other services that may be relevant and invites to events.

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to promote our business and services.



4.2.5 Complying with any requirement of law, regulation or a professional body of which we are a member

As with any provider of professional services, we are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.

- **Legal grounds: Legal obligation or legitimate interests**

This processing is necessary for us to comply with a legal obligation; for example, when conducting customer due diligence checks to comply with anti-money laundering regulations and, where we do not have a legal obligation, we have a legitimate interest in processing personal data as necessary to meet our regulatory or professional obligations.

We are continually looking for ways to help our clients and improve our business and services. Where agreed with our clients, we may use information that we receive in the course of providing professional services for other lawful purposes, including analysis to better understand a particular issue, industry or sector, provide insights back to our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings. To the extent that the information that we receive in the course of providing professional services contains personal data, we will de-identify the data prior to using the information for these purposes.

- **Legal grounds: Legitimate interests**

We have a legitimate interest in de-identifying data to help our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings, including by performing benchmarking and analysis.

4.3 Data retention

We retain the personal data processed by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulation).

In the absence of specific legal, regulatory or contractual requirements, our baseline retention period for records and other documentary evidence created in the provision of services is up to 10 years.

Personal data may be held for longer periods where extended retention periods are required by law or regulation and in order to establish, exercise or defend our legal rights.



4.3.1 When and how we share personal data and locations of processing

Further details about the processors (such as IT service providers) used by PwC and locations of processing are available upon request or check the annexures. We may use other organizations to help us deliver our services as agreed with our client on an engagement-specific basis.

5 Individuals who use our applications

We provide external users access to various applications managed by us. Such applications will contain their own privacy statements explaining why and how personal data is collected and processed by those applications. We encourage individuals using our applications to refer to the privacy statements available on those applications.

6 Individuals whose personal data we obtain in connection with providing professional services to our clients

6.1 Collection of personal data

Our policy is to collect only the personal data necessary for agreed purposes and we ask our clients only to share personal data with us where it is strictly needed for those purposes.

Where we need to process personal data to provide our services, we ask our clients to provide the necessary information to the data subjects concerned regarding its use.

We collect and use contact details for our clients in order to manage and maintain our relationship with those individuals. Please see the [Business contacts](#) section of this privacy statement for more information about our processing of this type of data.

Given the diversity of the services, we provide to clients, we process many categories of personal data, including:



- Personal details (e.g. name, age/date of birth, gender, marital status, country of residence);
- Contact details (e.g. email address, contact number, postal address);
- Financial details (e.g. salary, payroll details and other financial-related details such as income, investments and other financial interests, benefits, tax status); and
- Job details (e.g. role, grade, experience, performance information and other information about management and employees).

For certain services or activities, we may process special categories of personal data (such as in performing know your client checks and providing immigration and tax services, which involve us processing government identification documents that may contain biometric data or data revealing racial or ethnic origin or as part of an audit of an organization in the health sector).

Generally, we collect personal data from our clients or from a third party acting on the instructions of the relevant client. For some of our services, for example, when undertaking a due diligence review of an acquisition target on behalf of a client, we may obtain personal data from that target's management and employees or from a third party acting on the instructions of the target.

6.2 Use of personal data

We use personal data for the following purposes:

6.2.1 Providing professional services

We provide a diverse range of professional services. Some of our services require us to process personal data in order to provide advice and deliverables. For example, we will review payroll data as part of an audit and we often need to use personal data to provide global mobility and pensions services.

- **Legal grounds:** [Legitimate interests](#), [legal obligation](#), [public interest or consent](#)

This processing of personal data by us is necessary for the purposes of the legitimate interests pursued by us in providing professional services and our client in receiving professional services as part of running their organization and, in some cases, we have a legal obligation to provide the services in a certain way (e.g. statutory audit). Where we process special categories of personal data, we rely on a relevant public interest condition or consent.



6.2.2 Administering, managing and developing our businesses and services

We may process personal data in order to run our business, including:

- managing our relationship with clients;
 - developing our businesses and services (such as identifying client needs and improvements in service delivery);
 - maintaining and using IT systems;
 - hosting or facilitating the hosting of events; and
 - administering and managing our website, systems and applications.
- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to administer, manage and develop our business and services.

6.2.3 Security, quality and risk management activities

We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for example, automated scans to identify harmful emails. We monitor the services provided to clients for quality purposes, which may involve processing personal data stored on the relevant client file. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to client engagements. We collect and hold personal data as part of our client engagement and acceptance procedures. As part of our client and engagement acceptance, we carry out searches using publicly available sources (such as internet searches and sanctions lists) to identify politically exposed persons and heightened risk individuals and organizations and check that there are no issues that would prevent us from working with a particular client (such as sanctions, criminal convictions (including in respect of company directors), conduct or other reputational issues).

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to ensure network and information security, manage risks to our business and check the quality of our services.



6.2.4 Complying with any requirement of law, regulation or a professional body of which we are a member

As with any provider of professional services, we are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.

- **Legal grounds: Legal obligation or legitimate interests**

This processing is necessary for us to comply with a legal obligation; for example, when conducting customer due diligence checks to comply with anti-money laundering regulations and, where we do not have a legal obligation, we have a legitimate interest in processing personal data as necessary to meet our regulatory or professional obligations.

We are continually looking for ways to help our clients and improve our business and services. Where agreed with our clients, we may use information that we receive in the course of providing professional services for other lawful purposes, including analysis to better understand a particular issue, industry or sector, provide insights back to our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings. To the extent that the information that we receive in the course of providing professional services contains personal data, we will remove the personal data prior to using the information for these purposes.

- **Legal grounds: Legitimate interests**

We have a legitimate interest in de-identifying data to help our clients, to improve our business, service delivery and offerings and to develop new PwC technologies and offerings, including by performing benchmarking and analysis.

6.3 Data retention

We retain the personal data processed by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulation).

In the absence of specific legal, regulatory or contractual requirements, our baseline retention period for records and other documentary evidence created in the provision of services is 7 years.

Personal data may be held for longer periods where extended retention periods are required by law or regulation and in order to establish, exercise or defend our legal rights.



When and how we share personal data and locations of processing
Further details about the processors (such as IT service providers) used by PwC and locations of processing are available upon request and in annex. We may use other organizations to help us deliver our services as agreed with our client on an engagement-specific basis.

7 Others who get in touch with us

We collect personal data when an individual gets in touch with us with a question, complaint, comment or feedback (such as name, contact details and contents of the communication). In these cases, the individual is in control of the personal data shared with us and we will only use the data for the purpose of responding to the communication.

8 Personnel (partners, staff and contractors)

We collect personal data concerning our own personnel (partners, staff and contractors) as part of the administration, management and promotion of our business activities. Please refer to our HR privacy statement for information on why and how personal data is collected and processed in relation to your role with PwC.

9 Recruitment applicants

9.1 Introduction

This section of our privacy statement describes why and how we collect and use personal data in connection with our recruitment activities.

If your application is successful, we carry out pre-employment screening checks as part of our onboarding process. Depending on the role you have applied for, these checks may include criminal records checks.

9.2 Collection of personal data



We will collect personal data in connection with our recruitment activities as described below. Most of the personal data we collect as part of our recruitment process is provided by you such as:

- Contact details (name, email, telephone number);
- Areas of interest;
- Username and password to apply for a role;
- CV, experience, education, academic and professional qualifications;
- Information provided as part of interviews and assessments;
- Social mobility data as part our contextual recruitment practices;
- Diversity and equal opportunities data;
- Pre-employment screening information if your application is successful;
- Information about your and your immediate family's financial relationships if your application is successful; and
- Bank account details if your application is successful.
- We create personal data in connection with our recruitment activities such as:
 - Interview and assessment results and feedback; and
 - Offer details.

We may obtain personal data from third party sources such as:

- Recruitment platforms and websites including sources data from news articles, professional social media accounts, firm websites, professional representative bodies
- References from your named referees;
- Information from your referrer (where applicable);
- Verification of information provided during the recruitment process by contacting relevant third parties (for example, previous employers, education and qualification providers) or using publicly available sources (for example, to verify your experience, education and qualifications); and
- Information from social media sites that you are a member of about your engagement with our recruitment campaigns.

9.3 Use of personal data

We process personal data for our legitimate interests to attract and secure the best talent to work with us as follows:

- To attract talent and market opportunities at PwC including by arranging, hosting and participating in events, marketing and advertising opportunities and using recruiters to help find talent for us.
- To identify and source talent including by searching our existing talent pool and publicly available sources (such as social media and job websites of which you are a member).



- To process and manage applications for roles at PwC, evaluate you for open positions that match your interests and experience throughout the PwC network, manage your candidate profile, send you email notifications and other announcements, request additional information or otherwise contact you about your candidacy.
- To screen and select talent by evaluating your suitability for employment with PwC, including through interviews and assessments and conducting background checks.
- To hire and onboard talent by making an offer to successful applicants and carrying out pre-employment screening checks.
- To conduct statistical analyses and create reports including for example regarding usage of our career's websites, demographic analysis of candidates, reports on PwC recruitment activities, and analysis of candidate sourcing channels.
- To administer and manage our careers websites and communicate with you about careers at PwC.
- Any other purposes stated when you provide the information to PwC.

We may carry out criminal records checks for the following purposes:

- To comply with our legal obligation if any
- For our legitimate interest or that of a third party to carry out pre-employment screening including a full background and criminal records check, depending on the role: (i) to establish whether an applicant has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct; or (ii) to comply with government and public sector clearance requirements.

We collect and use information about race and ethnicity, religious and philosophical beliefs and health data for the following purposes:

- For our legitimate interest and reasons of substantial public interest
- For health and social care purposes, including to comply with our legal obligation to make reasonable adjustments (for example, as a result of the outcome of a pre-employment medical assessment).
- To identify or keep under review the existence or absence of equality of opportunity or treatment.
- If your application is successful, to provide information on relevant PwC support and access to relevant PwC networks.



9.4 Automated processing of personal data

9.4.1 Making an online application:

This stage includes screening related to academic performance. Responses to online questions are compared to predefined responses set for the relevant roles. Where the predefined responses are exceeded, applicants will progress automatically to the next stage of the recruitment process.

9.4.2 Online Assessments (Situational judgement tests and Game-based psychometric assessments):

This stage includes a series of online assessments, which involve solely automated decision-making. The online assessments you will be asked to complete have pre-defined correct or incorrect responses, which relate to requirements needed for the role. The predefined responses are based on data that indicates what good job performance at PwC looks like (informed by job analysis conducted with PwC staff and partners) in relation to these assessments. Your responses to the online assessment questions and overall assessment score will be compared to the predefined responses and scores set for the relevant roles. Applicants with an overall assessment score that exceeds that required for the relevant role will progress automatically to the next stage of the recruitment process.

9.4.3 Video interview:

This stage may include a video interview that may use automated decision-making. Video may be analysed by PwC recruitment system for a recommendation.

Applicants with high-recommended scores will progress directly to the next stage of the recruitment process. The video interviews of all other applicants will be subjected to human review to determine whether they should progress or not.

PwC will be carrying out the automated decision-making as it is necessary for entering into a contract (i.e. the potential contractual relationship between PwC and you as employer and employee). Using automated decision-making supports PwC to maintain a fair and objective selection process, whilst managing the significant volume of applications received for school and college leaver, undergraduate and graduate recruitment roles each year. The recruitment technology used by PwC enables a streamlined selection process, which assesses candidates on the behavioral qualities identified as important to a successful career at PwC.



9.4.4 Reviewing the automated decisions

You can ask us to review the outcome of any automated decisions by emailing our HR recruitment team at afr_afss_recruitment@pwc.com. Please include your candidate ID and your recruitment process stage when emailing.

9.5 When and how we share personal data and locations of processing

In addition to the general information about when and how we share personal data and locations of processing, personal data processed by us in connection with our recruitment activities may be transferred to:

9.5.1 Other PwC member firms

Your personal data will be provided to the PwC firm that has posted the position for which you are applying and other PwC member firm(s) where the role you are being considered for involves working with other PwC member firm(s) and to assist with their recruitment and employment activities (for example, if they are recruiting for a role that matches your interests and experience).

If you are applying to one of our university programmes, your application data may be reviewed by the university to which you are jointly applying

9.5.2 Third party organizations that provide applications/functionality, data processing or IT services to us, or that provide screening services to us

We use the products and services of third party organisations as part of the recruitment processes. The products and services we use differ depending on the role you apply for.

9.6 Data retention

We retain personal data processed in connection with our recruitment activities as follows:



If your application is successful, we will retain relevant personal data as part of your employee record and your talent pool account (if you choose to join our talent pool).

If your application is unsuccessful, we will retain and use the information you provided to PwC as part of your application for a reasonable period of time to deal with any matter which may arise in connection with your application, for purposes of contacting you regarding other employment opportunities and for our legitimate business purposes (for example, to make sure we do not contact an individual about a role they have already applied for) and for as long as you are a member of our talent pool (if you choose to join our talent pool).

10 Suppliers (including subcontractors and individuals associated with our suppliers and subcontractors)

10.1 Collection of personal data

We collect and process personal data about our suppliers (including subcontractors and individuals associated with our suppliers and subcontractors) in order to manage the relationship, contract, to receive services from our suppliers and, where relevant, to provide professional services to our clients. The personal data is generally business card data and will include name, employer name, phone, email and other business contact details and the communications with us.

10.2 Use of personal data

We use personal data for the following purposes:

10.2.1 Receiving services

We process personal data in relation to our suppliers and their staff as necessary to receive the services. For example, where a supplier is providing us with facilities management or other outsourced services, we will process personal data about those individuals that are providing services to us.



- **Legal grounds: Legitimate interests**

This processing of personal data by us is necessary for the purposes of the legitimate interests pursued by us in receiving services.

10.2.2 Providing professional services to clients

Where a supplier is helping us to deliver professional services to our clients, we process personal data about the individuals involved in providing the services in order to administer and manage our relationship with the supplier and the relevant individuals and to provide such services to our clients (for example, where our supplier is providing people to work with us as part of a PwC team providing professional services to our clients).

- **Legal grounds: Legitimate interests**

This processing of personal data by us is necessary for the purposes of the legitimate interests pursued by us in providing professional services and our client in receiving professional services as part of running their organization.

10.2.3 Administering, managing and developing our businesses and services

We may process personal data in order to run our business, including:

- managing our relationship with suppliers;
- developing our businesses and services (such as identifying client needs and improvements in service delivery);
- maintaining and using IT systems;
- hosting or facilitating the hosting of events; and
- administering and managing our website, systems and applications.

- **Legal grounds: Legitimate interests**

This processing is necessary for the purposes of the legitimate interests pursued by us to administer, manage and develop our business and services.



10.2.4 Security, quality and risk management activities

We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for example, automated scans to identify harmful emails. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to our suppliers. We collect and hold personal data as part of our supplier contracting procedures. We monitor the services provided for quality purposes, which may involve processing personal data.

- **Legal grounds:** [Legitimate interests](#)

This processing is necessary for the purposes of the legitimate interests pursued by us to ensure network and information security, manage risks to our business and check the quality of the services.

10.2.5 Providing information about us and our range of services

Unless we are asked not to, we use business contact details to provide information that we think will be of interest about us and our services. For example, industry updates and insights, other services that may be relevant and invites to events.

- **Legal grounds:** [Legitimate interests](#)

This processing is necessary for the purposes of the legitimate interests pursued by us to promote our business and services.

10.2.6 Complying with any requirement of law, regulation or a professional body of which we are a member

As with any provider of professional services, we are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.



- **Legal grounds: Legal obligation or legitimate interests**

This processing is necessary for us to comply with a legal obligation; for example, when conducting supplier due diligence checks and, where we do not have a legal obligation, we have a legitimate interest in processing personal data as necessary to meet our regulatory or professional obligations.

10.3 Data retention

We retain the personal data processed by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulation). Personal data will be retained about our contacts at our suppliers for as long as it is necessary for the purposes set out above (e.g. for as long as we have, or need to keep a record of, a relationship with a contact, which is for the duration of our relationship with a contact or their organization) and then deleted in line with our deletion and retention policies. Personal data may be held for longer periods where extended retention periods are required by law or regulation and in order to establish, exercise or defend our legal rights.

10.4 When and how we share personal data and locations of processing

Further details about the processors (such as IT service providers) used by PwC and locations of processing are available upon request or in Annexures. We may use other organizations to help us deliver our services as agreed with our client on an engagement-specific basis.

11 Visitors to our offices

We have security measures in place at our offices, including CCTV and building access controls.

11.1 CCTV

There are signs in our office showing that CCTV is in operation. The images captured are securely stored and only accessed on a need to know basis (e.g. to look into an incident). We use the CCTV images for the legitimate purposes of promoting security and safety of our



personnel and members of the public, preventing and detecting crime and establishing, exercising and defending legal claims. We may disclose CCTV images to law enforcement bodies as requested and permitted by data protection law.

CCTV recordings are typically automatically overwritten after a short period of time (between 21 and 60 days after being recorded) unless an issue is identified that requires investigation (such as a theft).

11.2 Visitor records

We require visitors to our offices to sign in at reception and keep a record of visitors for a short period of time. Our visitor records are securely stored and only accessible on a need to know basis (e.g. to look into an incident).

11.3 Guest WIFI

We monitor traffic on our guest WIFI networks using industry standard intrusion detection systems. This allows us to see limited information about a user's network behaviours but will include being able to see at least the source and destination addresses the user is connecting from and to. We cannot inspect any encrypted web pages and therefore do not have access to any information (personal or otherwise) that the user might share via these web pages.

12 Visitors to our website

12.1 Collection of personal data

Visitors to our websites are generally in control of the personal data shared with us. We may capture limited personal data automatically via the use of cookies and analytics tools on our website.

We receive personal data, such as name, title, company address, email address, and telephone and fax numbers from website visitors; for example, when an individual registers updates from us.

Visitors are also able to send an email to us through the website. Their messages will contain the user's screen name and email address, as well as any additional information the user may wish to include in the message.

We ask that you do not provide special categories of personal data (such as race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or



mental health; genetic data; biometric data; sexual life or sexual orientation; and, criminal records) to us when using our website.

12.2 Use of personal data

When you provide personal data to us, we may use it for any of the purposes described in this privacy statement or as stated at the point of collection (or as obvious from the context of collection), including:

- where you submit your contact details, unless we are asked not to, we may contact you with information about PwC's business, services and events, and other information, which may be of interest to you. Should visitors subsequently choose to unsubscribe from mailing lists or any registrations, we will provide instructions on the appropriate webpage, in our communication to the individual, or the individual may contact us by email to AFSS_NDPP_requests@pwc.com;
- to administer and manage our website, including to confirm and authenticate your identity and prevent unauthorized access to restricted areas of the site or premium content;
- to communicate with you in order to distribute requested materials or ask for further information;
- to personalize and enrich your browsing experience by displaying content that is more likely to be relevant and of interest to you;
- to sort and analyse user data (such as determining how many users from the same organization have subscribed to or are using our websites);
- to determine the company, organization, institution, or agency that you work for or with which you are otherwise associated;
- to develop our businesses and services, including aggregating data for website analytics and improvements;
- aggregating data to conduct benchmarking and data analysis including, for example, regarding usage of our websites;
- to conduct quality and risk management reviews;
- to understand how people, use the features and functions of our websites in order to improve the user experience;
- to monitor and enforce compliance with our terms, including acceptable use policies; and
- any other purposes for which you provided the information to PwC (such as to subscribe you to the updates you request).

Our websites do not collect or compile personally identifying information for sale to non-PwC parties for their marketing purposes. If there is an instance where your personal data may be shared with a party that is not a PwC member firm, you will be asked for their consent beforehand.



12.2.1 Third party links

Our website may link to third party sites not controlled by PwC and which do not operate under PwC's privacy practices. When you link to third party sites, PwC's privacy practices no longer apply. We encourage you to review each third-party site's privacy policy before disclosing any personally identifiable information.

12.3 Data retention

Personal data collected via our websites will be retained by us for as long as it is necessary (e.g. for as long as we have a relationship with the relevant individual).

13 Events

13.1 Introduction

This privacy statement describes why and how PricewaterhouseCoopers LLP ("PwC", "we", "us", or "our") collects and uses personal data in connection with our events and provides information about your rights as a user of the application ("you", "user" or "individual").

Personal data is any information relating to an identified or identifiable living person. This privacy statement applies to personal data provided to us, both by you or by others and any personal data created in connection with your use of the application. We may use personal data provided to us for any of the purposes described in this privacy statement or as otherwise stated at the point of collection.

When collecting and using personal data, our policy is to be transparent about why and how we process personal data. To find out more about our specific processing activities in connection with the application, please go to the relevant sections of this statement.

13.1.1 Security

We adhere to internationally recognized security standards. Our information security management system relating to client confidential data is independently certified as complying with the requirements of ISO/IEC 27001: 2013. We have a framework of policies, procedures and training in place covering data protection, confidentiality and security and regularly review the appropriateness of the measures we have in place to keep the data we hold secure.



13.1.2 Changes to this privacy statement

We recognize that transparency is an ongoing responsibility so we will keep this privacy statement under regular review.

This privacy statement was last updated 22 April 2020.

13.1.3 Data controller and contact information

If you have any questions about this privacy statement or how and why we process personal data, please contact us at:

Data Protection Officer
PricewaterhouseCoopers Sub-Saharan Francophone Africa
Email: AFSS_NDPP_requests@pwc.com

13.2 Collection of personal data

We will collect personal data in connection with your attendance at our events described below.

Personal data provided directly by you:

- Name
- Job title
- Company
- Email
- Telephone
- Dietary / accessibility requirements
- Guest details
- Other information specific to the event such as breakout session choices

13.3 Use of personal data

We will use your personal data to manage attendance at our events and to ensure that any special requirements that you request are communicated to any relevant 3rd party agents for



example we will share with venues and/or caterers any dietary requirements that you provide to us.

Our lawful basis for this processing is where you have provided your consent, and where it is necessary for legitimate interest pursued by us in ensuring your needs are met when attending our events.

13.4 When and how we share personal data and locations of processing

We will only share personal data with others when we are legally permitted to do so. When we share data with others, we put contractual arrangements and security mechanisms in place to protect the data and to comply with our data protection, confidentiality and security standards.

We share personal data processed in connection with the application as follows:

13.4.1 Third party organizations that provide applications/functionality, data processing or IT services to us.

We are part of a global network of firms and in common with other professional service providers, we use third parties to help us run our business and these third parties may be located in other countries.

We sometimes use third party organizations that provide venues and catering for us. Where we use an external venue to host an event or an external catering company, we will share any dietary requirements that you provide to us with the external venue and/or catering company so that we can provide suitable refreshments.

13.5 Data retention

We retain personal data processed in connection with the application for the purpose of managing your attendance at our events.



13.6 Individuals' rights and how to exercise them

You have certain rights over your personal data. Data controllers are responsible for fulfilling these rights. Where we decide how and why personal data is processed, we are a data controller.

Individuals' rights are the right of access to personal data, to rectification of personal data, to erasure of personal data / right to be forgotten, to restrict processing of personal data, to object to processing of personal data, to data portability, the right to withdraw consent at any time (where processing is based on consent) and the right to lodge a complaint with a supervisory authority.

Please see further information about these rights and how to exercise them below.

13.6.1 Right of access

You have the right to obtain confirmation as to whether we process personal data about you, receive a copy of your personal data held by us as a data controller and obtain certain other information about how and why we process your personal data (similar to the information provided in this privacy statement).

You may exercise this right by emailing us at AFSS_NDPP_requests@pwc.com. We will aim to respond to any requests for information promptly and in any event within the legally required time limits.

13.6.2 Right to rectification

You have the right to request for your personal data to be amended or rectified where it is inaccurate (for example, if you change your name or address) and to have incomplete personal data completed.

To update personal data submitted to us, please email us at AFSS_NDPP_requests@pwc.com. When practically possible, once we are informed that any personal data processed by us is no longer accurate, we will make updates, as appropriate, based on your updated information.

13.6.3 The right to erasure / right to be forgotten

You have the right to obtain deletion of your personal data in the following cases:

- the personal data are no longer necessary in relation to the purposes for which they were collected and processed;



- our lawful basis for processing is consent, you withdraw consent and we have no other lawful basis for the processing;
- our lawful basis for processing is that the processing is necessary for a legitimate interest pursued by us, you
- object to our processing and we do not have overriding legitimate grounds;
- you object to our processing for direct marketing purposes;
- your personal data have been unlawfully processed; and
- your personal data must be erased to comply with a legal obligation to which we are subject.

To request deletion of your personal data, please email us at AFSS_NDPP_requests@pwc.com

13.6.4 The right to restrict processing

You have the right to restrict our processing of your personal data in the following cases:

- for a period enabling us to verify the accuracy of the personal data where you have contested the accuracy of the personal data
- your personal data have been unlawfully processed and you request restriction of processing instead of deletion;
- the personal data are no longer necessary in relation to the purposes for which they were collected and processed but the personal data are required by you to establish, exercise or defend legal claims; and
- for a period enabling us to verify whether the legitimate grounds relied on by us override your interests (where you have objected to processing based on it being necessary for the pursuit of a legitimate interest identified by us).

To restrict our processing of your personal data, please email us at AFSS_NDPP_requests@pwc.com.

13.6.5 The right to object to processing

You have the right to object to our processing of your personal data in the following cases:

- our lawful basis for processing is that the processing is necessary for a legitimate interest pursued by us; and
- our processing for direct marketing purposes.

To object to our processing of your personal data, please email us at AFSS_NDPP_requests@pwc.com.



13.6.6 Right to data portability

You have a right to receive your personal data provided to us and have the right to send the data to another organization (or ask us to do so if technically feasible) where our lawful basis for processing the personal data is consent or necessity for the performance of our contract with you and the processing is carried out by automated means.

To exercise your right to data portability, please email us at AFSS_NDPP_requests@pwc.com.

13.6.7 Right to withdraw consent

Where we process personal data based on consent, individuals have a right to withdraw consent at any time. We do not generally process personal data based on consent (as we can usually rely on another legal basis). Where we rely on consent for processing, to withdraw your consent please email us at AFSS_NDPP_requests@pwc.com or, to stop receiving an email from a PwC marketing list, please click on the unsubscribe link in the relevant email received from us. Please see the “Use of personal data” section of this privacy statement for further details about our processing of personal data based on consent.

13.6.8 Complaints

We hope that you will not ever need to, but if you do want to complain about our use of personal data, please send an email with the details of your complaint to AFSS_NDPP_requests@pwc.com. We will look into and respond to any complaints we receive.



14 Security

We take the security of all the data we hold very seriously. We adhere to internationally recognized security standards and our information security management system relating to client confidential data is independently certified as complying with the requirements of ISO/IEC 27001: 2013. We have a framework of policies, procedures and training in place covering data protection, confidentiality and security and regularly review the appropriateness of the measures we have in place to keep the data we hold secure.

14.1 When and how we share personal data and locations of processing

We will only share personal data with others when we are legally permitted to do so. When we share data with others, we put contractual arrangements and security mechanisms in place as appropriate to protect the data and to comply with our data protection, confidentiality and security standards.

We are part of a global network of firms and in common with other professional service providers, we use third parties located in other countries to help us run our business. As a result, personal data may be transferred outside the countries where our clients and us are located. This includes to countries outside the European Union and to countries that do not have laws that provide specific protection for personal data. Personal data held by us may be transferred to:

14.1.1 Other PwC member firms

For details of our member firm locations, please [click here](#) or check in annexure

We may share personal data with other PwC member firms where necessary for administrative purposes and to provide professional services to our clients (e.g. when providing services involving advice from PwC member firms in different territories).

We store personal data on our or other PwC member firm servers in the EU, Singapore and the USA. IT support and services are provided by PwC India and PwC's IT Services company.

Our business contacts are visible to and used by other PwC member firms to learn more about a contact, client or opportunity they have an interest in (please see the [Business contacts](#) section of this privacy statement for more information about our processing of this type of data).



14.1.2 Third party organizations that provide applications/functionality, data processing or IT services to us

We use third parties to support us in providing our services and to help provide, run and manage our internal IT systems. For example, providers of information technology, cloud-based software as a service provider, identity management, website hosting and management, data analysis, data back-up, security and storage services. The servers powering and facilitating that cloud infrastructure are in secure data centres around the world, and personal data may be stored in any one of them.

Further details of these providers are included below.

Name	Role	Address
Digital Guardian Inc.	Endpoint USB blocking and data leakage prevention	860 Winter Street, Suite 3, Waltham, MA 02451 USA
Google Ireland Limited	Business applications (such as email, documents and calendar)	Gordon House, Barrow Street, Dublin 4, Dublin, D04 E5W5 Data centres located in a number of locations around the world (EU, Chile, Singapore, Taiwan, USA)
Hewlett-Packard	Cloud PC backup solution	3000 Hanover St, Palo Alto, California 94304-1112, USA
IBM United Kingdom Limited	Software and cloud services	P.O. Box 41, North Harbour, Portsmouth, Hants, PO6 3AU, UK
Introhive Services Inc	Customer relationship management	364 Argyle St, 3rd Floor, Fredericton, Canada, NB E3B 1T9



Microsoft Limited	Azure cloud services	Microsoft Campus, Thames Valley Park, Reading, RG6 1WG, UK
Oracle Corporation UK Limited	Software and cloud services	Oracle Parkway, Thames Valley Park, Reading, Berkshire, RG6 1RA, UK
Salesforce	Customer relationship management system	Salesforce.com EMEA, Village 9, Floor 26 Salesforce Tower, 110 Bishopsgate London, EC2N 4AY, UK

14.1.3 Third party organizations that otherwise assist us in providing goods, services or information

On certain client engagements, we may engage or otherwise work with other providers to help us provide professional services to our clients.

14.1.4 Our clients

Where we need to process personal data to provide professional services to our clients, we may share personal data in our deliverables (such as the reports we create).

14.1.5 Auditors, insurers and professional advisers

We have a statutory auditor and number of business insurance policies in place and we may need to share personal data with them for business & professional reasons, for example, in the event of an insurance claim or an audit. We use other professional advisers, for example, law firms, as necessary to establish, exercise or defend our legal rights and obtain advice in connection with the running of our business. Personal data may be shared with these advisers as necessary in connection with the products and services they have been engaged to provide.



14.1.6 Law enforcement or other government and regulatory agencies or to other third parties as required by, and in accordance with, applicable law or regulation

Occasionally, we may receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, to establish, exercise or defend legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.

14.2 Changes to this privacy statement

We recognize that transparency is an ongoing responsibility so we will keep this privacy statement under regular review.

This privacy statement was last updated in April 2020.

14.3 Data controller and contact information

We are generally controllers for the personal data we process; however, we may provide some services, such as payroll services, as a processor (in which case our client is the controller). If you have any questions about this privacy statement or how and why we process personal data, please contact us at:

Data Protection Officer
PricewaterhouseCoopers Sub Saharan Francophone Africa
Email: AFSS_NDPP_requests@pwc.com

14.4 Individuals' rights and how to exercise them

Individuals have certain rights over their personal data and controllers are responsible for fulfilling these rights.



Individuals' rights may include the right of access to personal data, to rectification of personal data, to erasure of personal data / right to be forgotten, to restrict processing of personal data, to object to processing of personal data, to data portability, the right to withdraw consent at any time (where processing is based on consent) and the right to lodge a complaint with a supervisory authority.

Please see further information about these rights, when they are available and how to exercise them below.

14.4.1 Your right of access to personal data

You have the right to obtain confirmation as to whether we process personal data about you, receive a copy of your personal data held by us as a controller and obtain certain other information about how and why we process your personal data (similar to the information provided in this privacy statement). This right may be exercised by emailing us at AFSS_NDPP_requests@pwc.com. We aim to respond to any requests for information promptly and in any event within the legally required time limits.

14.4.2 Your right to rectification / amendment of personal data

You have the right to request for your personal data to be amended or rectified where it is inaccurate (for example, if you change your name or address) and to have incomplete personal data completed.

To update personal data submitted to us, you may email us at AFSS_NDPP_requests@pwc.com or, where appropriate, contact us via the relevant website registration page or directly amend the personal details held on relevant websites or applications with which you registered.

When practically possible, once we are informed that any personal data processed by us is no longer accurate, we will make updates as appropriate based on your updated information.

14.4.3 Your right to erasure / right to be forgotten

You have the right to obtain deletion of your personal data in the following cases:



- The personal data are no longer necessary in relation to the purposes for which they were collected and processed;
- our legal grounds for processing is consent, you withdraw consent and we have no other lawful basis for the processing;
- our legal grounds for processing is that the processing is necessary for legitimate interests pursued by us or a third party, you object to our processing and we do not have overriding legitimate grounds;
- you object to our processing for direct marketing purposes;
- your personal data have been unlawfully processed; or
- your personal data must be erased to comply with a legal obligation to which we are subject.

To request deletion of your personal data, please email us at AFSS_NDPP_requests@pwc.com.

14.4.4 Your right to restrict processing

You have the right to restrict our processing of your personal data in the following cases:

- for a period enabling us to verify the accuracy of your personal data where you have contested the accuracy of the personal data;
- your personal data have been unlawfully processed and you request restriction of processing instead of deletion;
- your personal data are no longer necessary in relation to the purposes for which they were collected and processed but the personal data are required by you to establish, exercise or defend legal claims; or
- for a period enabling us to verify whether the legitimate grounds relied on by us override your interests where you have objected to processing based on it being necessary for the pursuit of a legitimate interest identified by us.
-

To restrict our processing of your personal data, please email us at AFSS_NDPP_requests@pwc.com.

14.4.5 Your right to object to processing

You have the right to object to our processing of your personal data in the following cases:



- our legal grounds for processing is that the processing is necessary for a legitimate interest pursued by us or a third party; or
- our processing is for direct marketing purposes.

To object to our processing of your personal data, please email us at AFSS_NDPP_requests@pwc.com.

14.4.6 Your right to data portability

You have a right to receive your personal data provided by you to us and have the right to send the data to another organization (or ask us to do so if technically feasible) where our lawful basis for processing the personal data is consent or necessity for the performance of our contract with you and the processing is carried out by automated means.

To exercise your right to data portability, please email us at AFSS_NDPP_requests@pwc.com.

14.4.7 Your right to withdraw consent

Where we process personal data based on consent, individuals have a right to withdraw consent at any time. We do not generally process personal data based on consent (as we can usually rely on another legal basis). Where we rely on your consent for our processing of your personal data, to withdraw your consent please email us at AFSS_NDPP_requests@pwc.com or, to stop receiving an email from a PwC marketing list, please click on the unsubscribe link in the relevant email. Please see the relevant “Use of personal data” sections of this privacy statement for further details about our processing of personal data based on consent.



15 Complaints

We hope that you will not ever need to, but if you do want to complain about our use of personal data, please send an email with the details of your complaint to AFSS_NDPP_requests@pwc.com. We will look into and respond to any complaints we receive.



16 ANNEXURES:

16.1 Annex-1 How we are structured

PwC is the brand under which the member firms of PricewaterhouseCoopers International Limited (PwCIL) operate and provide professional services. Together, these firms form the PwC network. 'PwC' is often used to refer either to individual firms, within the PwC network or to several or all of them collectively.

In many parts of the world, accounting firms are required by law to be locally owned and independent. Although regulatory attitudes on this issue are changing, PwC member firms do not and cannot currently operate as a corporate multinational. The PwC network is not a global partnership, a single firm, or a multinational corporation.

For these reasons, the PwC network consists of firms which are separate legal entities. The firms that make up the network are committed to working together to provide quality service offerings for clients throughout the world. Firms in the PwC network are members in, or have other connections to, PricewaterhouseCoopers International Limited (PwCIL), an English private company limited by guarantee. PwCIL does not practise accountancy or provide services to clients. Rather its purpose is to act as a coordinating entity for member firms in the PwC network. Focusing on key areas such as strategy, brand, and risk and quality, the Network Leadership Team and Board of PwCIL develop and implement policies and initiatives to achieve a common and coordinated approach among individual firms where appropriate. Member firms of PwCIL can use the PwC name and draw on the resources and methodologies of the PwC network. In addition, member firms may draw upon the resources of other member firms and/or



SSFA Network Data Protection Policy

Changing the way we think Personal data



secure the provision of professional services by other member firms and/or other entities. In return, member firms are bound to abide by certain common policies and to maintain the standards of the PwC network as put forward by PwCIL.

The PwC network is not one international partnership and PwC member firms are not otherwise legal partners with each other. Many of the member firms have legally registered names, which contain “PricewaterhouseCoopers”; however there is no ownership by PwCIL. A member firm cannot act as agent of PwCIL or any other member firm, cannot obligate PwCIL or any other member firm, and is liable only for its own acts or omissions and not those of PwCIL or any other member firm. Similarly, PwCIL cannot act as an agent of any member firm, cannot obligate any member firm, and is liable only for its own acts or omissions.



16.2 Annex - 2 - List of countries within PwC Sub Saharan Africa

The member firms of Francophone Sub-Saharan Africa region are highlighted in red

- Albania
- Algeria
- Andorra
- Angola
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Bermuda
- Bolivia
- Bosnia and Herzegovina
- Botswana
- Brazil
- British Virgin Islands
- Brunei Darussalam
- Bulgaria
- Cambodia
- **Cameroon (Republic of)**
- Canada
- Cape Verde
- Cayman Islands
- **Chad**
- Channel Islands
- Chile
- China
- Colombia
- **Congo (Democratic Republic of)**
- **Congo (Republic of)**
- Costa Rica
- **Cote d'Ivoire (Ivory Coast)**
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- **Equatorial Guinea**
- Estonia
- Fiji
- Finland
- France
- **Gabon (Republic of)**
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Guatemala
- **Guinea**
- Honduras
- Hong Kong SAR, China
- Hungary
- Iceland
- India
- Indonesia
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jordan
- Kazakhstan
- Kenya
- Kosovo
- Kuwait
- Kyrgyzstan
- Lao PDR
- Latvia
- Lebanon
- Liberia
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau SAR, China
- Macedonia
- **Madagascar**
- Malawi
- Malaysia
- Maldives
- Malta
- Mauritius
- Mexico
- Moldova
- Monaco (Principality of)
- Mongolia
- Montenegro
- Morocco
- Mozambique
- Myanmar
- Namibia
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Nigeria
- Norway
- Oman
- Pakistan
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Poland
- Portugal
- Puerto Rico
- Qatar
- Romania
- Russia
- Rwanda
- Saudi Arabia
- **Senegal**
- Serbia
- Sierra Leone
- Singapore
- Slovak Republic
- Slovenia
- South Africa
- South Korea
- Spain
- Sri Lanka
- eSwatini/Swaziland
- Sweden
- Switzerland
- Taiwan
- Tanzania
- Thailand
- Trinidad & Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks & Caicos Islands
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- Uruguay
- Uzbekistan
- Venezuela
- Vietnam
- West Bank & Gaza
- Zambia
- Zimbabwe



SSFA Network Data Protection Policy

Changing the way we think Personal data

