

PAIA INFORMATION MANUAL

Prepared in accordance with Section 51 of the Promotion of Access to Information Act, No. 2 of 2000 (as amended) ("PAIA" or "the Act") and the Protection of Personal Information Act, No. 4 of 2013 ("POPI") of the Republic of South Africa.

TABLE OF CONTENTS

1. PURPOSE	3
2. COMPANY OVERVIEW	3
3. INFORMATION REQUIRED UNDER SECTION 51(1)(a) OF THE ACT	3
4. SECTION 10 PAIA GUIDE	4
5. VOLUNTARY DISCLOSURE/AUTOMATIC AVAILABILITY	4
6. RECORDS HELD UNDER SECTION 51(1)(D) OF PAIA	4
7. SUBJECTS AND CATEGORIES OF RECORDS HELD BY DIGICERT	5
8. PROTECTION OF PERSONAL INFORMATION ACT 2013	7
9. DETAIL ON HOW TO MAKE A REQUEST FOR ACCESS	10
10. AVAILABILITY OF THE MANUAL	10
11. ANNEX 1 (FORM 2): REQUEST FOR ACCESS	12

1. PURPOSE

The purpose of this PAIA Information Manual (“PAIA Manual” or “Manual”) of DigiCert South Africa Proprietary Limited, a subsidiary of DigiCert, Inc. (collectively referred to as “DigiCert”), is to disclose the information required under section 51 of South Africa’s Promotion of Access to Information Act, No. 2 of 2000 (as amended) (“PAIA” or the “Act”).¹

This Manual also provides a brief overview of DigiCert’s privacy practices as required by the Protection of Personal Information Act, No. 4 of 2013 (“POPI”) . For a more extensive description of DigiCert’s privacy practices, please visit DigiCert’s Public Privacy Notice at <https://www.digicert.com/digicert-privacy-policy>.²

2. COMPANY OVERVIEW

DigiCert is a global provider of digital trust and operates as a digital certification authority. DigiCert provides scalable TLS/ SSL, IoT, and PKI solutions for identity and encryption, as well as enterprise-grade certificate management platforms, industry-knowledgeable customer support, and market-leading security solutions. DigiCert South Africa Proprietary Limited is a subsidiary of DigiCert, Inc., which is headquartered in the United States.

3. INFORMATION REQUIRED UNDER SECTION 51(1)(a) OF THE ACT

Head of Private Body/Information Officer	Michael Johnson, Director A. Eric Porter, Director
Postal Address	Floors 3, 4, & 5 Gateway Building Century Blvd & Century Way 1 Century City Cape Town, Western Cape 7441 South Africa
Street Address	Floors 3, 4, & 5 Gateway Building Century Blvd & Century Way 1 Century City Cape Town, Western Cape 7441 South Africa
Telephone Number	+1-800-896-7973
Fax Number	n/a
Email	support@digicert.com
Deputy Information Officer (to handle requests)	Aaron Olsen
Email address of Deputy Information Officer	privacy@digicert.com

¹ See PAIA at [Promotion of Access to Information Act \[No. 2 of 2000\] \(www.gov.za\)](http://www.gov.za).

² See *Section 51 Manual* content requirements at <https://accesstoinformation.co.za/PAIA/section-51-manual/>, which requires the information under POPI.

4. SECTION 10 PAIA GUIDE

Section 10 of PAIA requires the Human Rights Commission to compose and maintain a guide for those who wish to exercise any right contemplated by PAIA. Such form is entitled the *Guide on How to Use the Promotion of Access to Information Act of 2000* and may be accessed at the following link:

- https://inforegulator.org.za/wp-content/uploads/2020/07/PAIA-Guide-English_20210905.pdf

The Guide is also available at the office the Human Rights Commission at::

Postal Address: Private Bag 2700,
Houghton, 2041
Telephone Number: +27-11-877 3600
Fax Number: +27-11-403 0625
Website: www.sahrc.org.za

5. VOLUNTARY DISCLOSURE AND AUTOMATIC AVAILABILITY OF CERTAIN RECORDS

DigiCert does not have any categories of records which are automatically available without a person having to request access in terms of PAIA, except for information published on DigiCert's Public Privacy Notice located at <https://www.digicert.com/digicert-privacy-policy>. All other records at DigiCert require a formal request to access such records. For generally inquiries, please contact privacy@digicert.com.

No notice has been submitted by DigiCert to the Minister of Justice and Constitutional Development regarding the categories of records that are available without a person having to request access in terms of Section 52(2) of PAIA. However, the information on the website of the business and an end user's account platform is also automatically available without having to request access in terms of PAIA.

6. RECORDS HELD IN ACCORDANCE WITH OTHER LEGISLATION: SECTION 51(1)(D) OF PAIA:

Aside from PAIA, other legislation may provide that DigiCert must allow certain persons access to specific records. Records are available in terms of the list of legislation in Table 1, below, as amended from time to time. Due to the number of laws applicable to DigiCert, the list of legislation may not be exhaustive. Please note that the information will only be provided in accordance with the requirements stated in the relevant piece of legislation, and the accessibility of documents and records may be subject to the grounds of refusal as set out in this PAIA Manual, the relevant piece of legislation or other applicable law.

Table 1

<u>Reference</u>	<u>Act</u>
No. 75 of 1997	Basic Conditions of Employment Act
No. 53 of 2003	Broad-Based Black Economic Empowerment Act
No. 71 of 1991	Business Act
No. 71 of 2008	Companies Act
No. 130 of 1993	Compensation of Occupation Injuries and Diseases Act
No. 89 of 1998	Competition Act

No. 98 of 1978	Copyright Act
No. 19 of 2020	Cybercrimes Act
No. 36 of 2005	Electronic Communications Act
No. 25 of 2002	Electronic Communications and Transactions Act
No. 55 of 1998	Employment Equity Act
No. 68 of 1997	Identification Act
No. 95 of 1967	Income Tax Act
No. 38 of 1997	Intellectual Property Laws Amendment
No. 66 of 1995	Labour Relations Act
No. 85 of 1993	Occupational Health and Safety Act
No. 2 of 2000	Promotion of Access of Information Act
No. 4 of 2013	Protection of Personal Information Act
No. 194 of 1993	Trademarks Act
No. 63 of 2001	Unemployment Contributions Act
No. 30 of 1996	Unemployment Insurance Act
No. 89 of 1991	Value Added Tax Act

7. SUBJECTS AND CATEGORIES OF RECORDS HELD BY DIGICERT

General information about the categories of information DigiCert collects on data subjects can be accessed via the DigiCert Public Privacy Notice at <https://www.digicert.com/digicert-privacy-policy>. DigiCert also holds various other records that may relate to data subjects, the categories of which are as listed below. Please note that a requester does not have unlimited rights to access to these records—access to such records may be refused in accordance with sections 62 through 69 of the Act.

a. Companies Act Records

- (i) Documents of Incorporation
- (ii) Memorandum of Incorporation
- (iii) Minutes of meeting of the Board of Directors
- (iv) Resolutions of the Board of Directors
- (v) Records relating to the appointment of corporate officers

b. Financial Records

- (i) Accounting records
- (ii) Annual financial reports
- (iii) Annual financial statements
- (iv) Banking details and bank accounts
- (v) Debtors/Creditors statements and invoices

- (vi) Policies and procedures
- (vii) Tax returns

c. Income Tax Records

- (i) PAYE Records
- (ii) Documents issued to employees for income tax purposes
- (iii) Records of payments made to SARS on behalf of employees
- (iv) All other statutory compliance records, including:
 - i. VAT
 - ii. UIF
 - iii. Workmen's Compensation

d. Personnel Documents and Records

- (i) Accident books and records
- (ii) Address lists
- (iii) Disciplinary code and records
- (iv) Employee benefits arrangements rules and records
- (v) Employment contracts
- (vi) Forms and applications
- (vii) Grievance procedures
- (viii) Leave records
- (ix) Medical aid records
- (x) Payroll reports/wage register
- (xi) Salary records
- (xii) Standard letters and notices
- (xiii) Training manuals
- (xiv) Training records

e. Procurement Department

- (i) Standard terms and conditions for supply of services and products
- (ii) Contractor, client, and supplier agreements
- (iii) Lists of suppliers, products, services, and distribution
- (iv) Policies and procedures

f. Sales Department

- (i) Customer details
- (ii) Information and records provided by a third party
- (iii) Policies and procedures

g. Marketing Department

- (i) Advertising and promotional material
- (ii) Policies and procedures

h. Compliance and Audit Department

- (i) Audit reports
- (ii) Policies and procedures
- (iii) Risk management frameworks
- (iv) Risk management plans

i. IT Department

- (i) Disaster recovery plans
- (ii) Information technology systems and user manuals
- (iii) Policies and procedures
- (iv) System documentation and manuals

8. PROTECTION OF PERSONAL INFORMATION ACT 2013

The following information describes DigiCert’s privacy practices, as required by the Protection of Personal Information Act of 2013 (“POPI”) and disclosed herein in accordance with PAIA. For more information on DigiCert data processing practices, please see our DigiCert Public Privacy Notice available at <https://www.digicert.com/digicert-privacy-policy>.

a. Purpose of Processing Personal Information

DigiCert collects and processes personal information for legitimate business purposes, including:

- (i) To provide services and products that our customers have requested or purchased;
- (ii) To communicate with our customers regarding the services and products they have requested or purchased;
- (iii) To facilitate staff and business administration;
- (iv) To make group-wide strategic business decisions, particularly with respect to staffing, succession planning, remuneration and personnel deployment and assignment;
- (v) To manage vendor, partner, reseller and other third-party relationships;

b. Data Subject Categories and Personal Information

- (i) **Employee/Personnel Data:** Personal information related to DigiCert employees and personnel generated in the normal course of employment and staff and business administration.
- (ii) **Customer, Partner, Reseller, Vendor, and other Third-Party Data:** Personal information related to business representatives of our customers, partners, resellers, vendors and other third parties.

c. Categories of Personal Information We Collect and Process

<ul style="list-style-type: none"> • Business Contact Information 	First and last name, email address, postal address, telephone and fax number(s), IP address, usernames and related account information, job title, employer, and certain payment details.
<ul style="list-style-type: none"> • Validation Information 	DigiCert processes sensitive personal information on a limited basis, including government-issued identification (driver’s license, passport ID, or other) as part of our validation processes related to certificate services.
<ul style="list-style-type: none"> • Biometric Information 	DigiCert processes sensitive personal information on a limited basis, including government-issued identification as part of our validation processes and certain biometric information for our customers who choose to use our Remote Identity Verification (“RIV”) process. Where required, we obtain the data subject’s separate consent prior to processing their sensitive personal information.
<ul style="list-style-type: none"> • Employee Information 	We collect certain Personal Information related to our employees.
<ul style="list-style-type: none"> • Job Candidate Information 	We collect certain Personal Information related to job candidates.

d. Disclosures to Third-Parties

The personal information may be disclosed to the following categories of recipients for as long as necessary to effectuate the purpose of processing or as may be otherwise required by law:

- (i) Member entities of DigiCert Group for internal processing;
- (ii) Third-party vendors (processors/service providers) processing information on our behalf;

e. Trans-border Flows of Personal Information

Personal information may be transferred across borders to the United States, European Economic Area, Switzerland, India, Japan, and Australia, and to other locations where a DigiCert Group entity is established.

f. Security Measures to Protect Personal Information

DigiCert's technical and organizational controls align with industry standards and business needs to achieve appropriate levels of privacy and security. The following list of controls outlines DigiCert's minimum baseline of standard practices to safeguard data.

- (i) Policy and Document Management – DigiCert keeps, reviews annually at a minimum, and tests an Information Security Policy, Business Continuity Plan, Disaster Recovery Plan, and Incident Response Process. DigiCert maintains and updates as necessary an intra-group data sharing agreement and appropriate vendor Data Processing Agreements. In addition to publicly posted privacy notices applicable to DigiCert products and services, DigiCert also maintains and reviews/updates on an annual basis an internal Framework Privacy Policy, governing privacy standards and processes applicable to DigiCert.
- (ii) Network Security Controls – DigiCert's System Administrators ensure that publicly accessible information system components (e.g., public web servers) reside on separate sub-networks with separate physical network interfaces. DigiCert's System Administrators also ensure that controlled interfaces protecting the network perimeter filter certain types of packets to protect devices on DigiCert's internal network. Firewalls and boundary control devices are configured to allow access only to what is necessary to perform DigiCert's operations.
- (iii) Database Security Controls – All access (via system or directly by personnel) to DigiCert databases is logged and monitored for unauthorized changes. Data is encrypted in databases using an industry-recommended cipher, and direct access is limited to roles as specified by DigiCert's Information Security Policy and Certification Practices Statement.
- (iv) Access Controls and Authentication – All user interactions with DigiCert systems are traceable to the individual performing such actions and all users must be positively identified prior to being able to interact with DigiCert systems. DigiCert personnel must first authenticate themselves to DigiCert systems before they are allowed access to any components of the system necessary to perform their trusted roles and roles are defined by DigiCert's Certification Practices Statement and Information Security Policy. User accounts and other types of access to DigiCert computer systems must be approved in accordance with the User Access Policy. Both physical and logical controls, as outlined in applicable policies, to authorized individuals are reviewed periodically and, at minimum, yearly.
- (v) Personnel Controls – All DigiCert employees and other workers with access to DigiCert data and/or systems are subject to confidentiality agreements and are required to pass background checks and have specific, role-based training. DigiCert maintains and enforces policies and procedures for trusted roles, identification and authentication for each role, sanctions for unauthorized actions, separation of duties, employee badging, and immediate removal of system access for terminated employees/workers.

- (vi) Physical Security Controls – Access to every office, computer room, and work area containing sensitive information is physically restricted. All office doors have a lock, and all entrance doors to DigiCert facilities are always locked. These doors are accessible by an Access Card or other access control device, which is issued upon confirmation of a clean background check. DigiCert data centers, cages, and offices are monitored by CCTV. The secured cage requires biometric and dual custodian personnel for access. All access is logged.
- (vii) Vulnerability Management/Patching – Monthly scans are performed on all DigiCert assets using vulnerability detection tools. Systems requiring remediation are required to be patched within timelines defined by Global Security Operations. Timelines are based on the assigned Common Vulnerability Scoring System (CVSS) score. Critical and high vulnerabilities are patched within 72 hours or have a plan of action created, medium vulnerabilities are patched or have a plan of action created within 30 days, and low/information vulnerabilities are patched at DigiCert’s discretion.
- (viii) Comprehensive Internal Assessment – DigiCert performs an annual comprehensive risk assessment to identify all of the reasonably foreseeable internal and external threats to security, privacy, confidentiality, and integrity.
- (ix) Penetration Assessment/External Assessment – At least one third-party penetration assessment is conducted each year. DigiCert typically performs multiple penetration tests per year on code, infrastructure, and systems as well as completing red team assessments.
- (x) Training and Awareness – All employees and other workers are required to undergo annual privacy, security, and compliance training. Employees or others handling personally identifiable information and sensitive information receive additional training. All workers with access to DigiCert systems and/or data are required to adhere to policies and procedures for proper data handling, such as DigiCert’s Information Security Policy, Code of Conduct, and Acceptable Use Policy.
- (xi) Third-Party Access Controls – DigiCert’s contracts with third parties who may access DigiCert systems or data adequately address security and privacy requirements. These third parties are also subject to a privacy and security impact assessment and risks are mitigated prior to access.
- (xii) Data Protection in Storage and Transmission – All data stored in DigiCert systems is encrypted using an industry-recommended cipher. Likewise, all data transmitted within DigiCert systems worldwide is encrypted in transit using an industry-recommended cipher.
- (xiii) Storage, Retention, and Deletion – Information stored physically or electronically have the appropriate technical controls determined by the level of data classification. Information is deleted in accordance with our CP/CPS and applicable privacy notices.

9. DETAIL ON HOW TO MAKE A REQUEST FOR ACCESS

a. PAIA Requests

In accordance with section 50(1)(a) of PAIA, a requester may have a right to access their records if “that record is required for the exercise or protection of any rights.” Under certain circumstances, we may refuse access to such records.³ If we do refuse access, we will, to the extent that we are required, inform the requester as to the reasons why we refuse access.

³ See Chapter 4 of PAIA.

A request for access to information must be made by using the prescribed (by regulation) form. The form is located on the Information Regulator’s (South Africa) website at <https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-PAIA-Form02-Reg7.pdf>, and made available at the end of this Manual.

Access Fees

- The Deputy Information Officer will by written notice require each requester (other than a personal requester) to pay the prescribed request fee (if any) before further processing any request.
- The fee that the requester must pay to a private body is R140, provided that the requester may lodge and application to the court against the tender or payment of the request fee.⁴
- After the Deputy Information Officer has decided on the request, the requester will be notified in the required form. If the request is granted, then a further access fee must be paid for reproduction and for search and preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.
- The fee structure is available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za.


DigiCert has the right to reject any request for information submitted in terms of Sections 62 to 69 of the Act.

b. POPI Requests

Requesters may have rights under POPI to request access to **personal information** that we collect and process. For such requests, no fee is required. Email us at privacy@digicert.com to make such a request.

10. AVAILABILITY OF THE MANUAL

This PAIA Manual is made available as required by regulation and is available for inspection at its listed premises in Section 2 as well as on its website at <https://www.digicert.com/legal-repository>.



Signature of Head of Private Body

Mike Johnson

Name of Head of Private Body

04/17/2024

Date of Signature



Signature of Head of Private Body

Eric Porter

Name of Head of Private Body

04/17/2024

Date of Signature

⁴ Fee is subject to change. See [Section 54 | Fees - PAIA \(accesstoinformation.co.za\)](#).

Publication date of this manual: August 1, 2022

Next revision date of this manual: August 1, 2023

ANNEX 1: FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. Proof of identity must be attached by the requester.
2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The Information Officer

(Address)

E-mail address:

Fax number:

Mark with an "X"

Request is made in my own name

Request is made on behalf of another person.

PERSONAL INFORMATION									
Full Names									
Identity Number									
Capacity in which request is made <i>(when made on behalf of another person)</i>									
Postal Address									
Street Address									
E-mail Address									
Contact Numbers	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px;">Tel. (B):</td> <td style="width: 40%; padding: 2px;"> </td> <td style="width: 20%; padding: 2px;">Facsimile:</td> <td style="width: 20%; padding: 2px;"> </td> </tr> <tr> <td style="padding: 2px;">Cellular:</td> <td colspan="3" style="padding: 2px;"> </td> </tr> </table>	Tel. (B):		Facsimile:		Cellular:			
Tel. (B):		Facsimile:							
Cellular:									
Full names of person on whose behalf request is made <i>(if applicable)</i> :									
Identity Number									
Postal Address									

Street Address			
E-mail Address			
Contact Numbers	Tel. (B)		Facsimile
	Cellular		

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)

Description of record or relevant part of the record:	

Reference number, if available	
--------------------------------	--

Any further particulars of record	

TYPE OF RECORD
(Mark the applicable box with an "X")

Record is in written or printed form	
Record comprises virtual images <i>(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)</i>	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS
(Mark the applicable box with an 'X'?)

Printed copy of record <i>(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)</i>	
Written or printed transcription of virtual images <i>(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)</i>	
Transcription of soundtrack <i>(written or printed document)</i>	
Copy of record on flash drive <i>(including virtual images and soundtracks)</i>	
Copy of record on compact disc drive <i>(including virtual images and soundtracks)</i>	
Copy of record saved on cloud storage server	

MANNER OF ACCESS
(Mark the applicable box with an 'X'?)

Personal inspection of record at registered address of public/private body <i>(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)</i>	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format <i>(including transcriptions)</i>	
E-mail of information <i>(including soundtracks if possible)</i>	
Cloud share/file transfer	
Preferred language <i>(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)</i>	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED

If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.

Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a)	<i>A request fee must be paid before the request will be considered.</i>
b)	<i>You will be notified of the amount of the access fee to be paid.</i>
c)	<i>The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.</i>
d)	<i>If you qualify for exemption of the payment of any fee, please state the reason for exemption</i>
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication <i>(Please specify)</i>

Signed at _____ this _____ day of _____ 20 _____

Signature of Requester I person on whose behalf request is made

FOR OFFICIAL USE

Reference number:	
Request received by: (State Rank, Name And Surname of Information Officer)	
Date received:	

<i>Access fees:</i>	
<i>Deposit (if any):</i>	

Signature of Information Officer