

Data Security - In Office

For employees working in office. Please fill in the consent [form](#) after review.

Topics

- GDPR Introduction
- Why is Data Security important?
- Sensitive Data and PII
- External Data Security
 - Secure Platforms & Licenses
 - Storing Data
 - Login Authentication
- Internal Data Security
 - Data Usage (Purpose, Storage)
 - Limits to Access (Sharing Rules, G-Suite Editing Access)
 - Communication

GDPR Principles

To protect data at ACE

GDPR Principles

- GDPR stands for **General Data Protection Regulations**
- It is a **Pan-European** data protection law and applies to all ACE Markets.
- It exists to protect the data of ACE customers.

GDPR Principles

- There are 6 Principles that ACE must comply with:
 - 1) Lawfulness, Fairness and Transparency
 - 2) Purpose Limitation
 - 3) Data Minimisation
 - 4) Accuracy
 - 5) Storage Limitation
 - 6) Integrity and Confidentiality (Data Security)
- ACE abides by these principles as directed by ACE Amsterdam.
- The important one for all markets is **Principle 6 - Data Security**.

Principle 1: Lawfulness, Fairness, Transparency

Data must be collected and processed in a lawful, fair, and transparent manner with regards to the data subject. This includes the collection of data based on a lawful basis (consent, contract, legal obligation, vital interest, public task, or legitimate interest). The use of data must not breach any other laws and must be used in a fair way that is not detrimental, unexpected, or misleading. Information and communication concerning processing personal data must be easily accessible and easy to understand through clear and plain language. These values must be held when collecting personal information from the data subject/client. The client must be able to provide informed consent on the purpose, duration, and third parties that may access their data. To remain transparent with the data subject, you must state in your privacy policy the type of data you collect and the reason you collect it.

- What is ACE lawful basis?
Consent, contract
- Must not breach **laws**, within each market ACE must abide by national laws in addition to GDPR (usually GDPR is strictest)
- **Transparency in communication** means ensuring data subjects understand terms of contracts & data collection.

Principle 2: Purpose Limitation

There must be a purpose limitation to personal data so that it may not be processed further than the legitimate purpose. Further processing for purposes of the public interest, scientific or historical research, or statistical purposes are allowed. The data controller/processor must be clear about the purposes, record the purposes as a part of documentation obligations, inform individuals about the purpose and ensure that if data is used for purposes outside of those disclosed then this new use is also fair, lawful, and transparent.

- ACE must only process data limited by the **purpose**.
- ACE's purpose includes **selling products, servicing customers, maintaining productive effectiveness, raising capital for expanding operations**.

Principle 3: Data Minimisation

The data collected must be adequate, relevant, and limited to the purpose of collection. Data collection should not be excessive, but be sufficient to fulfil stated purpose and has a rational link to that purpose. There could exist a need to gather more data in the case that the purpose cannot be satisfied. The assessment of what data is needed should be based on the purposes of processing itself. Data should be deleted if it is deemed not relevant to fulfilling the purpose. Data minimisation applies to the collection, use, and sharing of data. The sharing of data should be minimized to the least sensitive possible.

- The data collected must be **adequate and relevant** to the purpose.
- It is important that data collection is **not excessive** → every data point should be tied to a purpose.

Principle 4: Accuracy

The data controller must consider whether it is necessary to periodically update the information to preserve the accuracy of the data. The inaccurate data must be deleted or rectified without delay. Customers must be able to express when their personal data is incorrect or misleading as there are obvious risks to the processing of incorrect data. The source and status of personal data must be clear. The data controller must also anticipate and consider any challenges to the accuracy of information. Historical records may be kept, as long as it is clear that it is historical (changing addresses, etc.) Opinions may be stored and are not necessarily inaccurate, as long as it is clear that it is an opinion.

- Data should be **updated** regularly to preserve accuracy.
- **Inaccurate** data should be rectified.
- **Historical data** can be kept but must be classified as historical.

Principle 5: Storage Limitation

Data must be stored in a form that makes it possible to identify data subjects for no longer than is necessary for the established purpose or processing. The data controller must think about and justify the duration that data is kept based on the purpose of this collected data. Relevant actions may include the establishment of a retention policy/schedule to comply with documentation requirements. The data should be periodically reviewed and erased or anonymised when it is not needed. Anonymisation is an alternative to deletion. The challenges to data retention must be considered, especially when it comes to erasure. This is a data protection principle that can be included in any data governance policies. To comply with GDPR, the organisation should document standard retention periods for different categories of information help, however some small organisations may be exempted from this documentation.

- ACE should not **store** data for longer than is necessary (ACE has obligations to local governments & KIVA to retain data)
- Data can be **anonymised** as an alternative to deletion.

Principle 6: Integrity & Confidentiality (Security)

The data must be appropriately secured, including protection against unlawful or unauthorised processing, damage, accidental loss. Measures taking may include appropriate authentication and encryption. The organisation may set technical or organisational measures to ensure the integrity and confidentiality. This protection principle will take into account the cost of implementation, the nature of the scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

- Data must be **securely** stored (from external and internal threats).
- May include organisational measures.

Principle 7: Accountability

The controller of this data must be able to be held accountable for their adherence to the data principles outlined. The data controller must have appropriate measures and records in place to demonstrate compliance.

- ACE must express **accountability** & demonstrate **compliance** with evidence.
- This may include technical and organisational measures.

Data Security

Introduction

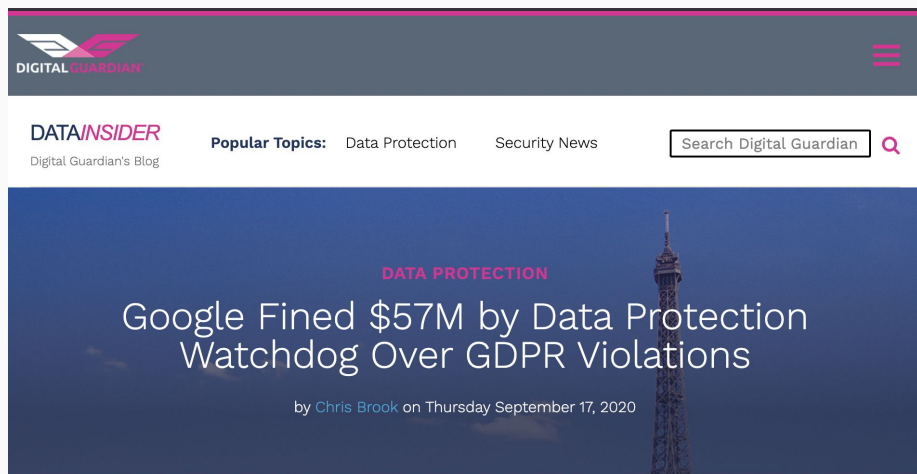
Data Security (Principle 6)

- Data security refers to making sure there is enough **protection of personal data**. This includes unauthorized access, processing, and damage.
- You need to keep your data secure from **external threats**, such as hackers.
- You also need to keep your data secure from **within your organisation** by putting in place guidelines for collecting, storing, and using data.

Why is it important?

1. The GDPR has strict **fin**es for when its principles are broken (up to 2% of a company's annual revenue)
2. Data breaches have consequences for the **wellbeing of customers**
3. Data breaches have consequences for the **reputation of ACE**

GDPR Fines in the News



The screenshot shows the Digital Guardian website. At the top left is the Digital Guardian logo. Below it is the 'DATA/INSIDER' section, which is the Digital Guardian's Blog. To the right of this are 'Popular Topics' for 'Data Protection' and 'Security News'. A search bar is located to the right of the popular topics. The main content area features a large blue banner with the text 'DATA PROTECTION' in pink, followed by the headline 'Google Fined \$57M by Data Protection Watchdog Over GDPR Violations' in white. Below the headline, it says 'by Chris Brook on Thursday September 17, 2020'. The background of the banner is a dark blue sky with the Eiffel Tower visible.

The French data protection authority said Monday that it has fined Google roughly \$57M - the biggest penalty yet under the new law - for failing to acknowledge how its users' data is processed.

Pinsent Masons > OUT-LAW > NEWS > BRITISH AIRWAYS FINED £20M

British Airways fined £20m over GDPR breach

OUT-LAW NEWS | 19 Oct 2020 | 3:52 pm | 4 min. read



British Airways (BA) has been fined £20 million by the UK's data protection authority over data security failings which enabled unauthorised access to be obtained to personal and payment card information relating to more than 400,000 of its customers.

Data Security for Customers

- When ACE sells their products to new individuals, it begins a customer relationship: this relationship is built on **trust**.
- Customers can expect ACE to manage their data in a responsible manner.
- If ACE does not uphold external and internal data security, it will break customer trust.
- This can negatively affect the customers, as their sensitive information can land in the hands of those with **malicious intent**.
- Consequently, **ACE's reputation will be damaged by word of mouth**. This will have a negative impact on future sales.

Sensitive Data & PII

Gaining Customer Trust

ACE Data Collection

- ACE **collects data from customers** such as: customer name, GPS location, payment history, household demographics, etc.
- ACE **uses this data** to:
 - Sell ACE products
 - Complete maintenance for sold ACE products
 - Secure financing from other organisations to sponsor loans
 - Measure ACE impact
- ACE's data collection & usage complies with GDPR Principles (ACE only collects the necessary data & uses it for business purposes)

Sensitive Data & Personally Identifiable Information (PII)

1. **Sensitive Data:** Some of the data that ACE collects is **sensitive** for the customer. This may include their loan status, amounts in arrears, current remaining balance.
2. **Personally Identifiable Information (PII)** is data that can uniquely identify a specific customer.
 - PII Examples are:
 - Full Name
 - Phone Number
 - Location
 - Social Security Number

Sensitive Data & Personally Identifiable Information (PII)

- When you **combine sensitive data with PII**, this can be used to tie particular behaviors to individuals.
 - For example, you know John Smith's full name, phone number, and the fact that he has 30EUR remaining balance on his loan.
 - This is information that may cause dangerous situations for the customer.
- For **within ACE**, it is often necessary to combine sensitive data with PII to conduct business
 - Need to know which customers live in which territory or what their loan status is.
- But the combination of sensitive data and PII should not be shared outside of ACE (unless absolutely necessary).

Examples of Personally Identifiable Information

| | Customer Owner | Customer Name | Sales Team | Territory | Current Remaining Balance | GPS Location (Latitude) | GPS Location (Longitude) |
|---|----------------|---------------|----------------|--------------|---------------------------|-------------------------|--------------------------|
| 8 | Lim Linda | John Smith | KH - ECOMMERCE | Kampong Thom | USD 105,00 | 13,11695400000000 | 103,17652900000000 |

Personally Identifiable Information

| | Customer Owner | Customer Name | Sales Team | Territory | Phone | Current Remaining Balance |
|---|----------------|---------------|----------------|--------------|--------------|---------------------------|
| 8 | Lim Linda | John Smith | KH - ECOMMERCE | Kampong Thom | 088 634 2891 | USD 105,00 |

Checklist: is this PII?

- ❑ Does this piece of information identify an individual customer or can it apply to more than one customer?
 - ❑ Example: GPS coordinates of a customer's house vs. territory
- ❑ If this information is shared out of ACE, could external parties locate or contact the customer?

If YES, then it is PII.

When do we use PII?

- There are certain activities at ACE for which we **include PII**. For example:
 - Completing maintenance for customers
 - Calling customers about loan payments
- However, these are scenarios that ACE **does not need to include PII**:
 - Creating a statistic on the number of customers in an area
 - Sharing data on our customer base with third parties (third parties may need general locations of the customers, but do not need to know full names or phone numbers).

PII and Customer IDs

- To protect the customer's sensitive data, ACE assigns a unique **Customer ID** to every customer that can replace PII.
- This unique ID can be used to create reports and share data on sales, service, and loan management with third parties.
- Now, if third parties get a hold of the data, they cannot tie this record to an individual customer.

| | Customer Owner <input type="checkbox"/> | Customer ID <input type="checkbox"/> | Sales Team <input type="checkbox"/> | Territory <input type="checkbox"/> | Current Remaining Balance <input type="checkbox"/> |
|---|---|--------------------------------------|-------------------------------------|------------------------------------|--|
| 8 | Lim Linda | 0011v00002ynJW7 | KH - ECOMMERCE | Kampong Thom | USD 105,00 |

Customer Trust

- By replacing PII, like a full name, with a unique Customer ID, ACE will protect the sensitive information of customers.
- This gains **customer trust**.

External Data Security

Protection from external threats

External Data Security

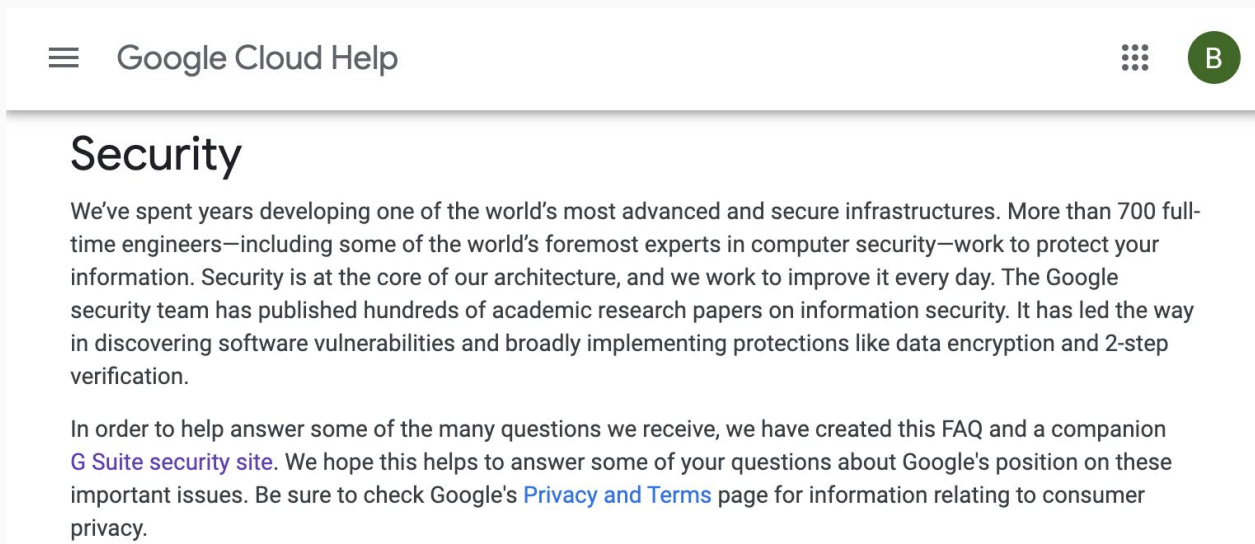
- Protecting data from external threats (outside of ACE activities)
 - Hackers who want to sell data
 - Malware
- External data security is built-in to most of ACE's activities
 1. Use of **secure platforms (G-Suite, Salesforce)**
 2. **Encryption** of data in ACE apps like the ACE Connect App.
 3. Preventing unauthorized access with **user authentication**

1. Secure Platforms

- ACE uses **G-Suite** and **Salesforce** to store the majority of data.
- G-Suite stores written reports for funding applications, sheets with customer data, information about ACE employees, ACE standard operating procedures, copies of contract templates.
- Salesforce stores data on ACE customers, sales, maintenance and service cases, stove usage.
- These two platforms are **committed to data security and protection.**

1. G-Suite Security Policies

- Data on G-Suite is stored in the secure Google Cloud



The screenshot shows the top navigation bar of the Google Cloud Help page. On the left, there is a hamburger menu icon followed by the text "Google Cloud Help". On the right, there is a grid icon and a circular profile icon containing the letter "B". Below the navigation bar, the word "Security" is displayed in a large, bold font. The main content area contains two paragraphs of text. The first paragraph discusses Google's investment in security infrastructure and the role of its security team. The second paragraph mentions a FAQ and a companion G Suite security site, and refers to Google's Privacy and Terms page.

☰ Google Cloud Help ☐ B

Security

We've spent years developing one of the world's most advanced and secure infrastructures. More than 700 full-time engineers—including some of the world's foremost experts in computer security—work to protect your information. Security is at the core of our architecture, and we work to improve it every day. The Google security team has published hundreds of academic research papers on information security. It has led the way in discovering software vulnerabilities and broadly implementing protections like data encryption and 2-step verification.

In order to help answer some of the many questions we receive, we have created this FAQ and a companion [G Suite security site](#). We hope this helps to answer some of your questions about Google's position on these important issues. Be sure to check Google's [Privacy and Terms](#) page for information relating to consumer privacy.

1. Salesforce Security Policies

< BACK TO HOME

Description

Salesforce.com uses a variety of methods to ensure that your data is safe, secure, and available only to registered users in your organization.

Resolution

Your data is secure with salesforce.com. Your data will be completely inaccessible to your competitors.

Salesforce.com utilizes some of the most advanced technology for Internet security available today. When you access our site using a supported web browser, Secure Socket Layer (SSL) technology protects your information using both server authentication and data encryption. When you log in, you will see a small lock icon at the bottom of your browser display, indicating that a secure connection has been established to our server.

Salesforce.com provides each user in your organization with a unique username and password that must be entered each time a user logs in. Salesforce.com issues a session "cookie" only to record encrypted authentication information for the duration of a specific session. The session "cookie" does not include either the username or password of the user. Salesforce.com does not use "cookies" to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs.

1. Data Outside of these Platforms

- When you take data from G-Suite or Salesforce and store it on an alternative platform (**personal laptop, hard drive, third party website**) → you are **no longer protected by security policies** from these platforms.
- If you really have to download data to your personal laptop for ACE activities there are a couple things you must do.

1. How to Protect Data on Personal Computers

1. If you are downloading customer data, ask yourself: do I need to include **PII** or can I use anonymised ID numbers instead?
2. After you have used the data, **upload the data back to G-Suite Drive.**
3. Once back on G-Suite Drive, **delete** the data files from your personal computer.

1. Platform Licenses

- As an ACE employee, you receive **licenses** to the ACE Platforms
 - name@africanenergy.com
 - Login to Salesforce
- These licenses are allocated to you based on your role and activities at ACE
- You should **not share your licenses with others** -- unless it is a group account (eg. Sales Team Taroworks account)

3. Login Authentication and 2FA

- Login Authentication refers to the **username and password** for your accounts
- Two Factor Authentication (2FA) requires you to fill in your username and password and subsequently authenticate your account using an **email code or text message**.
- 2FA is used in many companies and institutions as it provides the most data security.
 - Example: If your laptop is stolen, the thief will not be able to login to your account (even if you have saved your username and password) because they do not have access to your email or phone.

3. Password Requirements

- ❑ Passwords for your ACE accounts should be difficult to guess.
- ❑ For example, include both **lowercase and UPPERCASE** letters, include **numbers**, and **special characters** (!@#\$%^).
- ❑ It is very important to keep your passwords **private**, if you have trouble remembering your passwords you can write them down in a secret location.
- ❑ Your password must be **updated** every 4 months.

3. Phone Passwords

- If you use Salesforce, you **MUST** have a **password on your phone** too as this protects your 2FA.
- It is important that all **sales or maintenance agents** that access customer data from the field also have a **password on their phone**.

Internal Data Security

Internal company policies

What is internal data security?

- Internal data security is concerned with the **collection, storage, access, usage, and sharing** of data within the organisation.
- Different roles within ACE require access to different data.
 - Sales Manager need information on demos, prospects, and well-performing sales teams
 - Call Center agents need to know the phone numbers of different customers
- Data sometimes has to be **shared** across countries or departments to complete activities → this needs to be done in a secure way.
- Internal data security also relates closely to data privacy.

Internal Data Security at ACE

In this presentation, we will look at how you:

1. Access data
2. Store data
3. Share data

For both Salesforce and G-Suite. If you do not have a Salesforce or G-Suite account you may ignore those parts of the presentation.

Salesforce: Access to Data

Access to Data: Salesforce

- Roles/Positions at ACE have different access to data on SF.
- Data in SF is categorised into:
 1. **Objects:** a collection of columns and rows on a certain data object. Examples include Users, Opportunities, Cases, Energy Surveys.
 2. **Fields:** the columns on a data object. For Opportunities, these fields may include Opportunity ID, Customer Name, Quantity, Territory, Amount
 3. **Records:** rows or individual instances of a data object. For example Opportunity ID: 2738291, Customer Name: John Smith, Quantity 4, Territory: Maseru, Amount: 100USD

Access to Data: Salesforce

- The SF administrator controls your access to data using **profiles, permission sets, and sharing settings (defaults, sharing rules, role hierarchies)**
- 1. **Object** access is determined by your SF profile + permission sets for additional access individual users. Your access can be read only or you may have editing access.
- 2. **Field** access are applied by modifying profiles or adding more permissions

Access to Data: Salesforce

3. **Record** access is determined by:

- a. Organisational wide defaults
- b. Role hierarchies
- c. Sharing rules: automatic exceptions to org-wide defaults
- d. Manual sharing: additional permissions to records (can also be temporary access)

Access to Data: Salesforce

- The profiles, permission sets, and sharing rules not only determine what data you can **see**, but also what you can **do** with that data.
- Some permissions will include the ability to **edit, delete, or export data**.
- You may find yourself unable to download excerpts of data from Salesforce because your permission sets do not allow you to download data from that particular object, or including that particular field.

Access to Data: Salesforce Common Errors

1. You cannot see a **report** because you do not have access to the object it is based on.
2. You cannot see all of the customers **records** you expect to see.
 - a. You will not be able to view customers outside of your geographical area. However if you work in EA you will see both Uganda and Kenya.
3. You cannot see **components** on your dashboard.
 - a. This means the report on which the component is based has been altered so that one of the groupings is missing. For example, the component's x-axis was "Date of Sale" but this grouping was removed from the report. This is likely an error created when clicking into the report (see: SF Usage Guide).
4. More information in the SF Visualisation deck.

Salesforce: Storing Data

Saving Data on SF: Reports and Dashboards

- Salesforce saves reports & dashboards into folders.
- You can save into **public** & **private** folders.
- **Private Folders/Reports/Dashboards:** are only accessible to you. Use this when you want to get quick information from a report for yourself without having to share it with others.
- **Public Folders/Reports/Dashboards:** accessible to anyone in the organisation who's SF sharing settings allow them to see this information. If someone else opens this report/dashboard, they will only be able to see the data that pertains to them.

Saving Data on SF: Report Folders

Private reports are only visible to you.



If you want to share the report you made with others, save it in one of the folders in public reports.



Select

All Folders

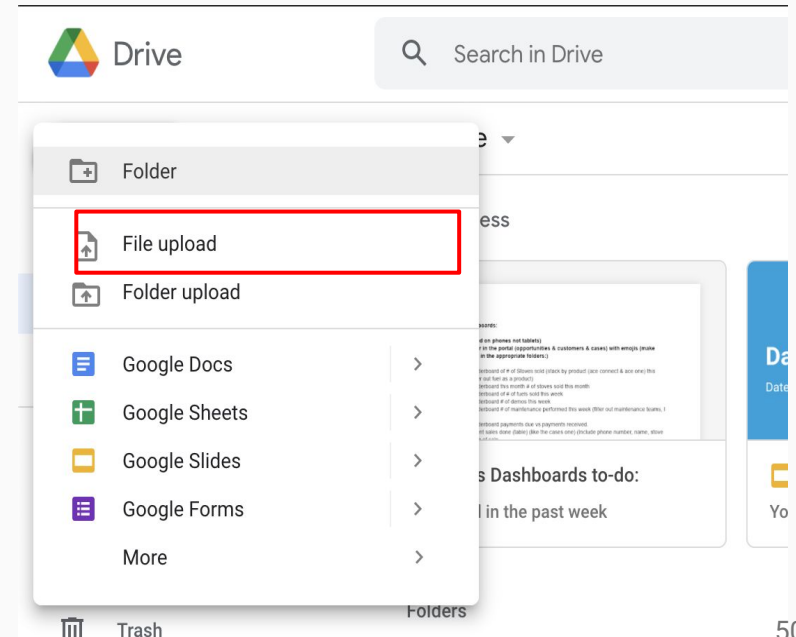
Search folders...

| | |
|-----------------|-------------------------------------|
| All Folders | Amarins |
| Created by Me | Baptiste |
| Shared with Me | Cambodia Call Centre Dashboard |
| Private Reports | Cambodia Reports |
| Public Reports | Cambodia Sales Reports |
| | CWB Report |
| | Dashboard Reports |
| | Dashboard Reports - Adoption |
| | Dashboard Reports Home Page |
| | Data Loader Reports |
| | Form Reports |
| | HealthChecks |
| | Hugh's Lesotho Reports |
| | Inventory Management Extracts |
| | <u>Job Target Reports - General</u> |
| | Lesotho Call Centre Dashboard |
| | Lesotho Customer Service |
| | Lesotho MFI Dashboard |
| | Lesotho Reports |
| | Loan Management Portfolio |
| | Loans |

New Folder Cancel Select Folder

Downloading Data from SF

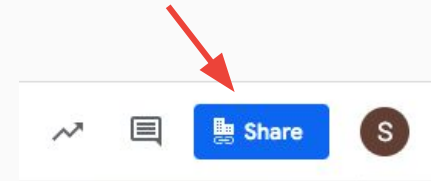
- On occasion you may need to **download data from SF** to share with your teams. (eg. List of Customers that need to be visited today)
- If you do need to download this data → **Save it to G-Drive and delete it from your personal computer.** If you do not have a G-Drive license then you may print it off from your personal computer and then delete the file.



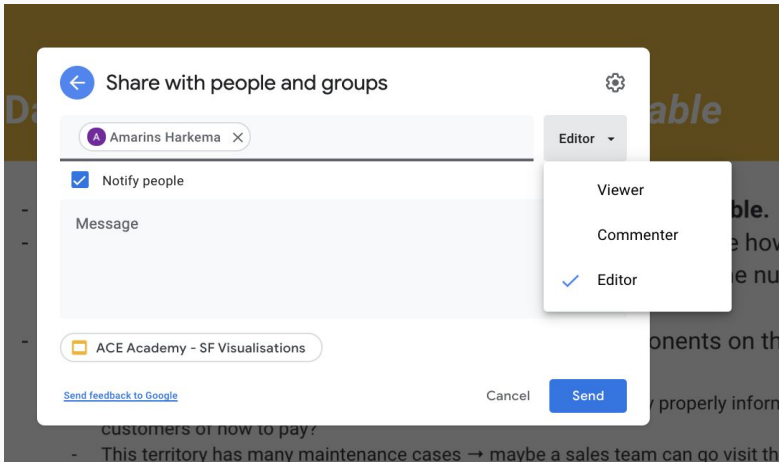
G-Suite: Access to Data

Access to Data: G-Suite

- On G Suite you can decide who gets **access to the files you have created**.
- You can add collaborators to your documents, presentations, spreadsheets, and so on.
- To do this, you should:
 - Select the **Share** button on your file.
 - Enter the **email addresses** of those whom you want to access your file.
 - Optional: add a message.
 - Select **send**.



Access to Data: G-Suite



- Once you have selected the name of the individual, you choose what **type of access** to give.
1. **Viewer**: can only see the document
 2. **Commenter**: can view the document and make comments on the side.
 3. **Editor**: can edit the document (including what the owner has written/created)
- Select **“Notify People”** to ensure that the individual gets an email.

Access to Data: G-Suite Sharing Files

Who has access to the files

The screenshot displays the 'Share with people and groups' interface in Google Drive. At the top, there is a search bar labeled 'Add people and groups'. Below it are tabs for 'All', 'Guests', and 'Members'. A list of users is shown with their profile pictures, names, email addresses, and roles. The roles are: Editor, Viewer, Editor, Editor, Viewer, and Viewer. At the bottom of the list is a 'Send feedback to Google' link and a 'Done' button. Below the list is a 'Get link' section with a link icon, the text 'African Clean Energy Anyone in this group with this link can view', a 'Change' link, and a 'Copy link' button.

| Name | Email | Role |
|----------------------|---------------------------------|--------|
| Shantal Martis (you) | shantal@afriancleanenergy.com | Editor |
| ACE Amsterdam | amsterdam@afriancleanenergy.com | Viewer |
| asaba habibu sadiki | | Editor |
| Babet Nieman | babet@afriancleanenergy.com | Editor |
| Claire Eunice Akello | claire@afriancleanenergy.com | Viewer |
| Daniel Walker | | Viewer |

Add people to share the files

Who can view, comment or edit the files

Option to copy a shareable link that you can distribute separately

Access to Data: G-Suite (Sharing Rights)

An editor, commenter or viewer is able to:

| | Share or unshare | Edit content directly | Add comments |
|-----------|------------------|-----------------------|--------------|
| Editor | ✓ | ✓ | ✓ |
| Commenter | | | ✓ |
| Viewer | | | |

Access to Data: G-Suite (Shared Drive)

The previous slides only refers to one or different separate files. When managing folders on Google drive (which contains numerous files), other access levels apply. The roles are the following:

- **Manager:** can view, edit, move, or delete items, as well as manage team member access and permissions.
- **Content manager:** can view, comment on, edit, and add content. A content manager cannot add or modify team member permissions.
- **Contributor:** can add items, but can't move or delete items--although they can restore a deleted item from the Team Drive trash.
- **Commenter:** can only comment.
- **Viewer:** can only view.

To learn more about these access levels, click [here](#).

Access to Data: G-Suite Drive

Who has access to the folders

Manage members

Add people and groups

| | | |
|--|--|-----------------|
| | Shantal Martis (you) shantal@afriancleanenergy.com | Manager |
| | ACE Amsterdam amsterdam@afriancleanenergy.com | Viewer |
| | Babet Nieman babet@afriancleanenergy.com | Content manager |
| | Claire Eunice Akello claire@afriancleanenergy.com | Viewer |
| | Daniel Walker daniel@afriancleanenergy.com | Viewer |
| | Dominik Berg dominik@afriancleanenergy.com | Viewer |

[Send feedback to Google](#) **Done**

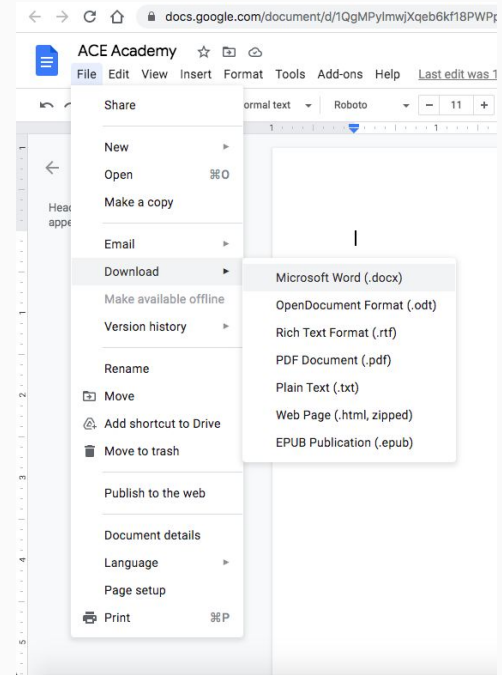
Add people to share the folders

Who can manage or view the folders

G-Suite: Storing Data

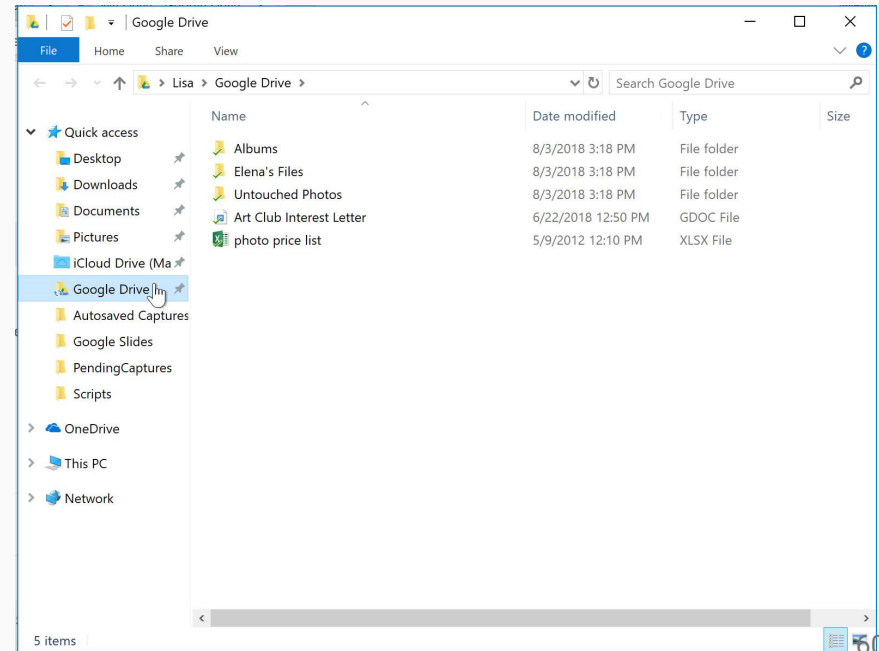
Saving Data: Downloading

- Sometimes you may need to download files from your drive, for instance when you want to attach a PDF in an email.
- When you do, make sure to **delete** the file from your personal computer once you are done using the downloaded version.



Saving Data: Desktop

- G-Suite, in particular G-drive, can also be used on your desktop.
- Here, you should also pay attention to stored data that are sensitive e.g. customer data. If you have files that contain such work related data, do not keep it on your desktop.



Communication of Data

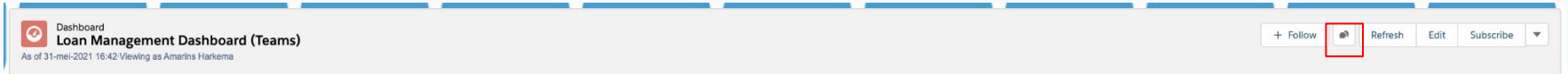
How do we share and communicate data within ACE?

General Communication

- Every market has their own best practices when it comes to communication: WhatsApp, Gmail, Google Chat, etc.
- Communication at ACE can include discussing sensitive information of customers or employees (customer names, loan status, etc.)
- Therefore, when sharing or discussing sensitive customer/employee data, you must use the **G-Suite tools (Gmail & Google Chat)** whenever possible, as this communication is secured.

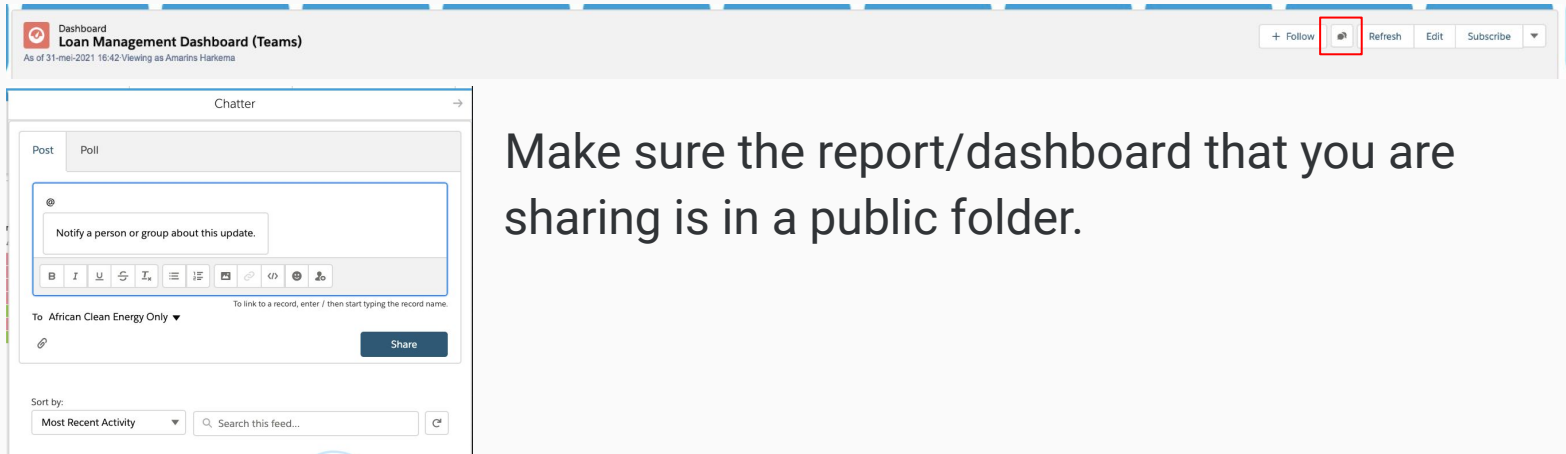
Communication of Data outside of ACE

- When sharing data with third parties, follow these **3 steps**:
 1. Review the [checklist](#) on PII → is it necessary to include PII in this document? Replace it with unique IDs if possible.
 2. Are you sharing the data within the company? Share using Secure Platforms
 - a. On Salesforce: @mention the user in the report or dashboard



Communication of Data (3 Steps)

2. Are you sharing the data within the company? Share using Secure Platforms
 - a. On Salesforce: @mention the user in the report or dashboard



Dashboard
Loan Management Dashboard (Teams)
As of 31-mei-2021 16:42 Viewing as Amarnis Harkema

+ Follow @ Refresh Edit Subscribe

Chatter

Post Poll

@
Notify a person or group about this update.

B I U L Undo I* Bold Italic Link Unlink Attachments

To African Clean Energy Only ▼

Share

Sort by: Most Recent Activity Search this feed...

Make sure the report/dashboard that you are sharing is in a public folder.

Communication of Data (3 Steps)

2. Are you sharing the data within the company? Use secure platforms.
 - b. Sharing on G-Suite?



On G-Suite, you can share data and information using the “Share” button in the top right corner.

Then follow the steps as described in the [“Internal Data Security”](#) section of this presentation.

Communication of Data (3 Steps)

3. Are you sharing data with **third parties** (government, NGO, partner)?
 - a. Repeat checklist for PII
 - b. Make the third party sign contracts on data privacy
 - i. Contract should call for the deletion of data once the purpose has been fulfilled
 - ii. Contract should state that third party will abide by data protection policies
 - c. Send the data via Gmail.

What to include in this report?

If in doubt... ask!

Sharing data?

Contracts with third parties?

References to other information

- [Video of the Data Security Presentation](#)
- [Data Security Consent Form for Management and Office Positions](#)
- [Data Security Presentation for In-Field Agents](#): a simplified presentation detailing the importance of accurate data input, sharing data via WhatsApp, etc.
- [Data Security Consent Form for In-Field Agents](#): make sure the teams that you manage agree to this form
- Data Security [Poster](#)