The [AWS whitepaper](https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf) (shared on the previous page) lists five (5) main things they say you can do with their tools to ensure compliance with GDPR requirements for processing data containing "Personally Identifiable Information" (PII) which could possibly be used to identify a specific individual:

1.  grant different permissions to different people for different resources

2.  require Multi-Factor-Authentication (MFA)

3.  use API-Request Authentication

4.  use geo-restriction (also known as "geo-blocking")

5.  create and provide trusted users with *temporary* security credentials

In no more than 250 words, reply to the following:

Pick an item from the above list and write a "model" policy statement on how and why to concretely implement it for a (fictitious or real) organization.

Type your response in the text field and submit it to the dropbox.

At Biotechs’R’Us, multi-factor-authentication (MFA) will be used by any statistician accessing clinical trial data, prior to its general release.

**Who:**Anyone with access to clinical trial data. This is ideally limited to only the statisticians working on the data, but may include any other employee deemed necessary for an applicable reason as determined by the Biotechs’R’Us CEO.

**What:** Doctors notes, patient outcome, patient response, clinical trial raw data and any other data related to a program noted as “Confidential to Biotechs’R’Us”.

**When**: Until the data and trial outcome has been announced to the general public in a press release.

**Where:**Data will only be accessed directly from a company computer logged into the local network, or a company computer logged in remotely via virtual private network (VPN).

**Why:**Critical decisions are made based on the outcome of these trials, and therefore require the utmost care in keeping the data secure. Decisions on whether to continue or terminate a program, which directly impact the direction of Biotechs’R’Us are extremely sensitive and will not be made publicly available until the company deems them ready for release.

**How**: MFA will be setup for each individual program. A user will be required to create a unique password for the specific program. At anytime a user wishes to access the data, they will be required to enter their password, which will prompt the system to send a unique key to their company email. The user will be required to enter this key into the database to gain access.