NINJIO GDPR 5-EPISODE SERIES: WHAT WE COVER.

THE BASIC PREMISE OF GDPR AS IT RELATES TO PEOPLE – OR AS GDPR CALLS THEM, "DATA SUBJECTS"

- What you do with a data subject's information should be what they would expect you would do with it.
- You need to protect their data with appropriate security measures.
- When you process data subject information, you need to do it in a way that is transparent, doesn't break the law, and is done so fairly.
- If there comes a point when you don't need a person's data, you should delete it.
- If inaccuracies exist in your data, you must fix it.
- If there is data in your system that you don't need and never use, you need to eliminate it from your system. This is known as "Data Minimalization." As an example of this is, if you are collecting the physical address of a person at a company, and you never use their physical address for any reason, that field in the database should be removed, and that data deleted.
- Data Subjects have several rights under GDPR. The overall premise of their rights is that they know exactly what you are doing with their information, that they can control what you do with their information, and that they can ask you to remove their information if they don't want you to have it. Which you must do. Free of charge.

HERE ARE THE SPECIFICS BEHIND THE DATA SUBJECTS CONCEPT:

- EU Citizens can ask, and have the right to know, what you are using their information for. They can ask for copies of the information that you have, which you must provide to them.
- EU Citizens can ask what your justification is for having their information, why you have it, and how long you plan to keep it. You must be able to answer these questions.
- If EU Citizens have asked for their information and it's not accurate, they can request that you to fix it, which you must do as quickly as possible.
- An EU Citizen can request that you "forget" them; a concept that is also known as "the right to be forgotten." In this instance you must delete ALL of their information from ALL of your systems. There are exceptions to this rule such as if you need their data in order to fulfill services that the data subject wants to keep receiving (i.e. Health Insurance)
- EU Citizens have the right to "information portability" which means that if they request their information, you need to provide it in a format that can be imported into another system. An example of information that is not portable would be giving them a print-out of their information. The print-out would not likely be importable into another system. Alternatively, giving them their information in a .csv file would likely be acceptable.
- EU Citizens can ask that their data not be used for marketing.

- EU Citizens have the right to understand how their information is being processed. For example, if a University is deciding ~~on~~ whether to further an admissions application to the next step, and that is done ~~all~~ through software without human intervention, the applicant can request that a human look at their information for consideration of further advancement, and you must comply with this request.
- For any and all of these requests, though it may take you hours to comply, and at great expense, you cannot pass on the expense to the EU Citizen. It must be done at no cost to them.
- For any or all of these requests that the EU Citizen makes, you have 30 days to comply and communicate back to them.

WHAT THE "DATA CONTROLLERS" (TYPICALLY A COMPANY IN POSSESSION OF EU CITIZENS INFORMATION) MUST DO:

- Data Protection, Data Security, and Data Privacy "By Design" – The clear majority of today's developers, develop the application first, and figure out how to secure it second. From now on, you should build a design with security and privacy at the core of the application and build your functionality around that.
- When you are using 3rd Party processors, you must obtain updated contracts to ensure the 3rd party processor has implemented the GDPR measures that may be applicable to them. Do your due diligence and figure out how seriously they are taking GDPR.
- Once you have all your policies and measures in place, they must get documented properly, such that you can demonstrate being compliant to a "Regulator" in the event of an audit.
- If you are a particular type or size of company operating outside of the EU, but regularly do business inside of the EU, you may need to appoint an EU representative.
- If you are a controller who has an excess of 250 employees, or have particular types of data, you will need to keep records of processing~~,~~ which can be accessible to the regulator at a moments' notice.
- Uh-oh. You've been breached. You now have 72 hours to inform the regulator, and if it is a high-risk breach, you may also need to disclose the breach to the data subjects whose information was breached.
- If you are a large company dealing with a lot of different types of PII (Personal Identifiable Information), you must assign someone as your "Data Protection Officer."

WHAT HAPPENS IF YOU CHOOSE NOT TO COMPLY:

- It can get ugly… *really* ugly. The fines can reach as high as 4% of global annual revenue or "global annual turnover" as stated in the GDPR documentation.
- The amount of the fine will vary greatly based on a myriad of factors, such as: Are you ignoring GDPR intentionally? Is the data you process valuable? Is there a lot of it? For example, if the data-subject is asking you to "forget them" and you refuse… that is a very big fine. Best advice: Become GDPR compliant.