NINJIO

2820 Townsgate Road
Suite 101
Westlake Village, CA 91361

Phone: +1 805 864 1999
Email: info@ninjio.com
Website: www.ninjio.com

GDPR

CLICK PLAY FOR EPISODE #3

NINJIO has developed a unique 5-episode series on GDPR designed to give end-users a broad understanding of what GDPR is, and the rules that will apply to data-subjects (people) and data-controllers (usually companies). As you've come to expect from NINJIO, the series is done all through storytelling, emotionally engaging the end user.

IF YOU'D LIKE TO SEE ALL OF THE TOPICS OF GDPR THAT WE COVER IN OUR 5-EPISODE SERIES, DOWNLOAD HERE.

PDF

WHAT'S COVERED IN THE 5 EPISODE SERIES:

EPISODE 1

General Data Protection Regulation (GDPR) is for companies both inside the European Union and outside the E.U.—such as American companies that frequently do business with organizations within the E.U.

GDPR applies to any personal data as it relates to people, aka 'data subjects'.

GDPR went into effect May 25, 2018, which was necessary because the last prior data protection regulation came out in 1995.

GDPR applies to 'data controllers'—organizations that have relationships with data subjects, and 'data 'processors'—organizations that work for data controllers and process personal data on the data controllers' behalf.

EPISODE 2

Data controllers and data processors need to keep minimal data.

Data controllers and data processors need to make sure their data is accurate. They need to secure it, and they need to keep it only as long as it's absolutely necessary.

People, or as GDPR calls them—data subjects – have rights with regard to their personal data and what you know about them. These rights must be honored.

EPISODE 3

The processing of personal data needs to be lawful, fair and transparent.

What's done with data subjects' personal data should be expected by them.

Data controllers and data processors must verify their data accurately. Team staff members may be required and should continually make updates whenever and wherever necessary, deleting data that's no longer needed—which is another GDPR mandate.

Effective security measures must be in place, such as firewalls, e-mail content filtering, automated software updates, and security awareness training program.

EPISODE 4

Data subjects have a right to know how you're going to use their data. They can ask for justification as to why you need it, and how long you're going to keep it. They can also request a copy of the data you have on them, which you are required to provide.

Data subjects have the right to request any mistakes in their data be rectified; which must be done in a timely manner.

A data subject's 'right to be forgotten' refers to their right to request their information be deleted. Exceptions to this rule do exist, however.

'Data portability' means a person's data must be given to them in a "machine-readable" format.

Data subjects can demand their data not be used for profiling or direct marketing.

People have the right not to be subjected to decision making as a result of automated processing. If a computer makes a decision that creates a material effect, the data subject has the right to say "I'd like a human being to look at that, as well."

No fees can be charged to a data subject for requesting any of the above. And data processors or controllers have one month to respond to any inquiries.

EPISODE 5

Data controllers must be able to demonstrate they are GDPR compliant, which means having appropriate polices in place and adhering to them.

Due diligence must be taken in vetting third party processors. The correct types of contracts must be used when partnering with them, and these contracts will likely need to be amended or revised to reflect GDPR requirements.

Every European Union member has a 'Data Protection Regulator.' In the event of a breach, this person must be notified within 72 hours. If the breach is particularly bad, or high risk, the data subjects themselves may need to be informed.

If your company is of a certain size or type, and you are not established in the EU, you may need to appoint an EU representative.

Depending on the amount and type of data your company deals with, you may need to appoint a 'Data Protection Officer.'

Failure to adhere to any of these rules could result in fines of up to 4% of gross revenue.