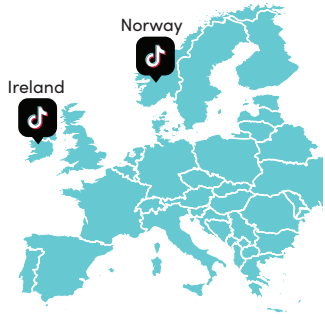
Project Clover

setting new standards in data security in Europe

At TikTok, we're going beyond existing regulations by introducing industry-leading measures to further strengthen our data security and protections in Europe.

Project Clover is a programme to create a reinforced protective environment for our European user data, consisting of a number of different innovative elements:

Data stored in Europe:



TikTok's user data is currently stored securely in the US, Singapore and Malaysia. We are now opening three new data centres in Ireland and Norway, which will become the default storage location for our European data. Our first Irish data centre is already online and we've started migrating European data to the centre. Our other two centres are under construction and will come online next year. These data centres represent a total investment of **€1.2 billion annually.**

We have already started storing the personal data for our EEA/UK users by default in a designated secure area known as the European Enclave, hosted in the interim in the US.

Independent third-party oversight:

We are pleased to announce that **NCC Group will oversee, check, and verify our data controls and protections, monitor data flows, provide independent verification and report any incidents.** NCC Group will provide multiple security services, including 24/7, 365 day security monitoring of the security gateways we are building around our European data, and security assessments of the TikTok platform itself. This independent oversight will supplement our already robust access approval process. NCC Group is a leading global cybersecurity and resilience provider, trusted by 14,000 clients worldwide. They are headquartered in the UK, with offices across Europe.

Stephen Bailey, Global Director of Privacy at NCC Group, said: "We're proud that TikTok has recognised NCC's cyber security track record and expertise and chosen us as the independent third-party security provider on this project. Our objective scrutiny, monitoring and assurance means platform users in Europe and the UK can have confidence in the enhanced data security standards that TikTok is setting, which go above and beyond European regulatory requirements."

Project Clover

setting new standards in data security in Europe

Enhanced data controls and restrictions:

We are building new security gateways that will form a secure barrier around our European data. NCC Group will co-manage these security gateways, which includes monitoring access requests and enforcing our access controls. **The security gateways will provide additional checks and protections and restrict data access even further, including no access to restricted data stored in the new European data enclave from employees in China.**

Restricted data is widely defined and includes all personal data of EEA/UK users unless it falls within three exceptions. By way of example, restricted data includes a user's real name (if collected), email address, phone number, IP address, and user-generated content which is set to an audience of "only me", etc. All personal data of EEA/UK users by default will be defined as "restricted data" unless the data is shared publicly by the user, or is aggregated, de-identified data, or needs to flow across our platform to ensure interoperability, e.g., information about a user's block lists, privacy settings, comments a user chooses to share, etc.

Privacy - enhancing technologies:

We are also working with NCC Group on building privacy-enhancing technologies (PETs) into these already robust procedures. This includes pseudonymisation of data that may need to flow for global interoperability, so that an individual cannot be identified without additional information, aggregation of individual data points into large data sets and differential privacy to prevent linking of relevant information to particular individuals. NCC Group will perform continuous validation of the efficacy of our PETs.

TikTok