# Committee Guide: **ECOSOC**

Europäische Schule RheinMain
The European School

Forum: United Nations Economic and Social Council (ECOSOC)
Issue: *Protecting individual rights to privacy in the digital age*
Chairs: Frederick Fink, Lili Rummel

**Table of Contents:**

Honorable Delegates and most esteemed administrative Staff at MUNESRM 2021,

We are more than delighted to welcome you to the United Nations Economic and Social Council – ECOSOC at MUNESRM 2021.

This Committee Guide should inform you and prepare you for the topics that will be debated at our upcoming conference:. We feel it is of the highest importance for delegates and chairs to be prepared to have a fruitful debate. In addition to reading this committee guide thoroughly and attentively, we recommend detailed research on your assigned country and information regarding the topic of discussion. To effectively debate, it is also essential to familiarize yourself with the Rules of Procedure. As this is only a short and brief Committee Guide, due to the current circumstances, we recommend you to check out the sources we attached for you in this Committee Guide.

# Key Terms

Data privacy:

Data privacy is the right of a citizen to have control over how personal information is collected and used. Data protection is a subset of privacy.

# General Overview

It is undoubted that the world's civilization is currently living through an era of digital fusion and technological accelerated development that increasingly presents itself in our daily lives. Now, about 4.6 billion worldwide individuals are active users of the internet. Technological advancement has not only made it easier to use modern information and communications technologies. Still, it has also increased entities, such as companies, governments, or even individuals, to partake in many data collection processes. These may constitute violations of human rights, and the right to privacy, which becomes an increasingly important matter, as more and more of such data is collected, potentially for future sharing or processing. Many times, this all happens without explicit and informed consent of individuals.

Edward Snowden, for example, was able to leak information from the National Security Agency (NSA) to the media in 2013. This event was only the start of a large number of precarious scandals where citizens found out the government had taken unauthorized information from them, which shocked and shaped the legislation and usage of the internet. Through them, the exploitation of the individual's digital actions has been disclosed.

Firstly, should governments have access to the individual citizen's data? To what extent should it be able to regulate its citzen's information?

Each type of government structure has enacted certain regulations in response to what extent and under which circumstances they are able to access citizen's data. However, are these regulations acting in the citizen's best interests? On one hand data can be useful for national statistics and even to curb the spread of the pandemic: the more a government knows about who went where, the easier it is to control the spread of the Covid-19 virus. On the other hand, this can pose a problem when considering the third principle of the Universal Declaration of Human Rights 'The right to life, liberty, and personal security.'. It is very important for global governments to outline under which circumstances and to what extent they should collect the data of citizens to ensure a peaceful future.

# Past actions

Past actions include the involvement of the UN, relevant resolutions, treaties, and events. The UN had only become active on the issue in the past years, as most of the problems arose. Following the concern of the UN General Assembly on this issue, the OHCHR created a report on digital privacy, which was presented in September 2014 and further discussed on the resolution of the General Assembly in December 2014. Furthermore, there have been multiple panels in the Human Rights Committee on this issue.

Following the resolution submitted to the General Assembly in 2014, several deeds have been taken:

- The OHCHR asked member states to review previous procedures and legislation regarding surveillance. This would mean that states are ensuring the following of the UDHR. Not all states have yet reviewed this as there are still international legislations that are not in accordance with the right of digital privacy.
- The FBI has also taken the initiative by wanting to monitor emerging threats through social media
- Outside the UN, attempts have taken place, such as the US forming a system called VANISH
- In 2017, Canada introduced the "Canada's Anti-Spam Law" that required everyone who sends email for commercial purposes to get explicit subscriber consent for receiving the emails in the first place.
- In 2018, the European Union introduced the "General Data Protection Regulation." This regulation outlines how consumer data can be collected, analyzed, transferred, and stored.
- Google announces that sites are required to use an HTTPS protocol in 2018 to contribute to a more secure Internet

- In 2020, California's Consumer Privacy Act (CCPA) got into effect. It defines its residents' personal data rights, allowing them access to their personal data and giving them agency over how data is collected, sold, and disclosed.

## Timeline of events:

A timeline that does not start from 2013 onwards can be found here (more thorough overview):

- European Commission
- International Network of Privacy Law Professional
- ECOSOC Helimun 2018
- Munsih.nl
- The Appreciation Engine

## Major parties and Their Views:

**The United States of America (USA):**

The United States was the central party when the Edward Snowden issue arose, as they were and still are working on preventing such a national problem from rising again. The United States government has been known to be collecting records of basic forms of communication, such as phone calls. In contrast to its European counterparts, the United States does not have one data privacy framework or directive. Instead, several states have introduced their framework and bills to and are at an all-time high. After California's Consumer Privacy Act passed in 2018, multiple states proposed similar legislation to protect citizens in their states.

**The European Union:**

Opposite to the United States, the European Union possesses over a single data privacy framework or directive. In 2018, the European Union introduced the "General Data Protection Regulation": "the toughest privacy and security law in the world". Though the regulation was passed and drafted by the European Union, it imposes obligations onto worldwide organizations, so long as they target or collect data related to people in the EU.

**The People's Republic of China/Authoritarian Regimes:**

China is the major party in internet censorship worldwide. Its citizens are strictly monitored in and outside of the domestic internet platform through espionage and facial identification. However, its government is currently ratifying its "Personal Information Protection Law",

which closed its seeking-opinion period on November 19, 2020. When the draft PIPL gets passed, China will finally have a central and universal governing law on protecting personal information. Along with the Cybersecurity Law implemented in 2017 and the Data Security Law, the PIPL is regarded as a major milestone in China's legislative efforts to establish a set of comprehensive regulation around data.

**The United Kingdom:**

The United Kingdom was affected by prominent hacker attacks. They were the prime subject to Project 415, and the UK has billions of phone calls hacked every year. In 2018, the British government introduced the Data Protection Act in 2018. It controls how personal information is used by Organisations, businesses or the government. Furthermore, citizens have the right to find out what information the government and other organisations store about them.

**Latin America:**

The GDPR has provided the necessary momentum for Latin American countries to update their existing laws governing data protection. As data transcends international borders, these developments are relevant to any organisation that does business in the region, particularly as recent trends suggest that data protection authorities are becoming increasingly active in enforcing data protection legislation in Latin America. Organisations that have adopted a GDPR standard across their business should take note of, and update its procedures in relation to, any local requirements that diverge from the GDPR (for example, data subject access request response time) once the final legislation has been released.

**Africa:**

There are currently 17 countries in Africa that have enacted comprehensive personal data protection legislation.In addition, the African Union (AU), adopted the AU Convention on Cybersecurity and Data Protection (AU Convention) in June 20142. However, the AU Convention has not currently taken effect as it has, to date,not been ratified by 15 out of the 54 AU member jurisdictions3. Nonetheless, the AU Convention does provide a personal data protection framework which African countries may potentially transpose into their national legislation, and encourages African countries to recognise the need for protecting personal data and promoting the free flow of such personal data,mtaking global digitalisation and trade into account

## Further sources:

- European Commission
- International Network of Privacy Law Professional
- ECOSOC Helimun 2018
- Munsih.nl
- The Appreciation Engine
- Congressional Research Service
- Privacy is Paramount
- Latin American Data Protection Law