**Federal State Autonomous Educational Institution of Higher Education**
**PEOPLES' FRIENDSHIP UNIVERSITY OF RUSSIA NAMED AFTER PATRICE LUMUMBA**
**RUDN University**

**Law Institute**
Educational Division

COURSE SYLLABUS

# Data Regulation and Protection in Digital Age

(Course title)

**Recommended by the Didactic Council for the Education Field**

40.03.01 Law

field of studies / speciality code and title

**The course instruction is implemented within the professional education programme of higher education:**

Bachelor of Laws (LLB)

higher education programme profile/specialisation title

**2026**

## 1. COURSE GOAL(s)

The main purpose is to familiarize with the basic rules of law governing the legal support of information security, to study of the conditions for the implementation of information security within the legal framework, to study of innovative digital solutions applicable in the field of information security

## 2. REQUIREMENTS FOR LEARNING OUTCOMES

Mastering the course is aimed at the Bachelor's students' formation of the following competencies (part of competencies):

*Table 2.1. List of competences that students acquire through the course study*

| Competence Code | Competence descriptor | Competence formation indicators (within this course) |
|---|---|---|
| PC-1 | Can draft regulatory acts, formulate legal norms for various levels of rulemaking and areas of professional activity. | PC-1.1. Identifies the societal need for legal regulations of public relations in a particular area as well as gaps and conflicts in the current legislation and has the tools to overcome and eliminate them; |
| PC-3 | Can engage in law enforcement, is capable of having the functions and authority to ensure security, law and order, to protect human and civil rights and freedoms | PC-3.3. Knows and has mastered the ways and methods of informing and protecting the rights and freedoms as well as the interests of citizens and organizations protected by law; |

## 3.COURSE IN HIGHER EDUCATION PROGRAMME STRUCTURE

The course refers to the elective component of (B1) block of the higher educational programme curriculum.

Within the higher education programme students also master other (modules) and / or internships that contribute to the achievement of the expected learning outcomes as results of the course study.

*Table 3.1. The list of the higher education programme components/disciplines that contribute to the achievement of the expected learning outcomes as the course study results*

| Competence Code | Competence descriptor | Previous courses/modules* | Subsequent courses/modules* |
|---|---|---|---|
| PC-1 | Can draft regulatory acts, formulate legal norms for various levels of rulemaking and areas of professional activity. | Comparative Constitutional Law and Justice<br>Comparative Administrative Law and Justice<br>Comparative Criminal Law<br>Computer Science<br>International Private Law<br>Civil and Arbitration Procedure | Legal Design<br>Legal Tech: Advanced Course<br>Workshop "Procedural Documents in Civil Cases"<br>Work Experience (Pre-graduation)<br>Internship |
| PC-3 | Can engage in law enforcement, is capable of having the functions and | Computer Science<br>Criminal Law | Legal Design<br>Legal Tech: Advanced Course |

| Competence Code | Competence descriptor | Previous courses/modules* | Subsequent courses/modules* |
|---|---|---|---|
| | authority to ensure security, law and order, to protect human and civil rights and freedoms | | Work Experience (Pre-graduation) Internship |

* - filled in based on the competency matrix

## 4. COURSE WORKLOAD AND ACADEMIC ACTIVITIES

1) The total workload of the course is 3 credits (108 academic hours)

*Table 4.1. Types of academic activities during the periods of higher education programme mastering* ***(full-time training)****

| Types of academic activities | | TOTAL, academic hours | Semester / Module | | | |
|---|---|---|---|---|---|---|
| | | | D | E | F | G |
| *Contact academic hours* | | *32* | | *32* | | |
| Lectures (LC) | | 16 | | 16 | | |
| Seminars (workshops/tutorials) (S) | | 16 | | 16 | | |
| *Self-studies* | | *58* | | *58* | | |
| *Evaluation and assessment (exam or pass/fail grading)* | | *18* | | *18* | | |
| **Course Workload** | academic hours | **108** | | **108** | | |
| | credits | **3** | | **3** | | |

* - must be completed in case of implementation of the program in extramural of study

## 5. COURSE CONTENTS

*Table 5.1. Course contents and academic activities types*

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| Legal regulation of relations in the area of information security. | Topic 1.1. Types and kinds of information security. Subjects to information security relations. | Information security encompasses various types, including confidentiality (preventing unauthorized access), integrity (protecting data from modification), and availability (ensuring timely access). Kinds of information security further include network security, application security, cloud security, and physical security of data carriers. Subjects of information security relations are individuals, legal entities, state bodies, and public associations that generate, store, transmit, or protect information. | LC, S |
| | Topic 1.2. Federal, regional and local information security laws. | Federal laws establish the fundamental framework for information security, such as Russia's Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection" and No. 152-FZ "On Personal Data." Regional laws adapt federal regulations to local conditions, often addressing data localization within specific territories or regional cybersecurity incident response. Local laws (municipal level) may govern access to municipal information systems, local data handling by schools or hospitals, and public Wi-Fi security ordinances. | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | Topic 1.3. The main international acts regulating the sphere of information security. | Key international acts include the Council of Europe's Budapest Convention on Cybercrime, which harmonizes cybercrime laws and mutual legal assistance procedures. The GDPR (EU General Data Protection Regulation) sets binding standards for personal data protection and cross-border data transfers, influencing non-EU countries. Other important instruments are the Shanghai Cooperation Organisation's International Information Security agreements, the African Union Convention on Cyber Security and Personal Data Protection, and various UN resolutions on responsible state behavior in cyberspace. | LC, S |
| | Topic 1.4. Information law: concept, subjects (participants) and objects. | Information law is a branch of legal system regulating social relations arising from the creation, collection, processing, storage, protection, and dissemination of information. Subjects (participants) include information producers (authors, media), information holders (state bodies, companies), information consumers (citizens, organizations), and regulatory authorities (Roskomnadzor, data protection agencies). Objects of information law are information itself (as an intangible asset), information rights, information systems, information technologies, and information security measures. | LC, S |
| | Topic 2.1. The concept of state secrets, legal regulation. | State secrets are statutorily protected information in the sphere of military, foreign | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | | policy, economic, intelligence, and counter-intelligence activities, the disclosure of which could harm national security. Legal regulation in Russia is primarily governed by the Law of the Russian Federation No. 5485-1 “On State Secrets,” which defines the list of classified information, clearance procedures, and liability for unauthorized disclosure. Similar frameworks exist abroad, such as the US Classified Information Procedures Act (CIPA) and the UK Official Secrets Act. | |
| Legal regulation to ensure the state secret and trade secret regime | Topic 2.2. The state secret regime. | The state secret regime establishes a system for classifying information into degrees of secrecy (e.g., “Top Secret,” “Secret”), granting access based on clearance levels, and protecting classified documents. It mandates special procedures for handling, storing, transmitting, and destroying state secrets, including physical security measures, personnel screening, and non-disclosure agreements. Violation of the state secret regime results in criminal, administrative, or disciplinary liability, with penalties ranging from fines to imprisonment. | LC, S |
| | Topic 2.3. The concept of trade secrets, legal regulation. | A trade secret is confidential business information (e.g., manufacturing processes, customer lists, pricing formulas) that has commercial value because it is not generally known and is subject to reasonable protection measures by its owner. Legal | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | | regulation in Russia is based on Federal Law No. 98-FZ “On Trade Secrets,” which defines the rights and obligations of trade secret holders and employees. International frameworks include the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which requires member states to protect undisclosed information. | |
| | Topic 2.4. The trade secret regime. | The trade secret regime requires the owner to take “reasonable steps” to maintain secrecy, including implementing access restrictions, confidentiality agreements with employees and contractors, and marking documents as “Trade Secret.” It also regulates the legal consequences of lawful acquisition (e.g., independent discovery or reverse engineering) versus unlawful misappropriation (theft, espionage, breach of contract). Judicial remedies for trade secret violations include injunctions, damages, and, in some jurisdictions, criminal penalties for industrial espionage. | LC, S |
| | Topic 2.5. The practice of legal regulation and protection of trade secrets in foreign countries. | In the United States, the Defend Trade Secrets Act (DTSA) of 2016 created a federal civil cause of action for trade secret misappropriation, complementing state-level Uniform Trade Secrets Act (UTSA) laws. The European Union’s Trade Secrets Directive (2016/943) harmonizes civil remedies across member states, while Germany and France have specific criminal | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | | provisions for trade secret theft. Many Asian jurisdictions, such as Japan (Unfair Competition Prevention Act) and China (revised Anti-Unfair Competition Law), have strengthened trade secret protection through enhanced evidentiary rules and increased damages. | |
| Legal regulation of blockchain in Russia and foreign countries. | Topic 3.1. Historical aspect of the formation of blockchain technologies in the legal field. | Blockchain emerged with Bitcoin's whitepaper in 2008, initially impacting legal fields through cryptocurrencies and anti-money laundering (AML) regulations. By the mid-2010s, legal scholars and practitioners began exploring blockchain for smart contracts, digital notarization, and evidence authentication (e.g., timestamping). The formation period saw the first legislative responses, including state laws in Arizona and Vermont recognizing blockchain signatures and smart contracts as legally valid. | LC, S |
| | Topic 3.2. Blockchain and information security are the main drivers for the development of the legal business. | Blockchain provides tamper-proof, auditable records that enhance information security, reducing the need for traditional intermediaries like title companies or escrow agents. Law firms increasingly adopt blockchain for secure client communication, immutable document storage, and automated conflict checking via distributed ledgers. The combination of blockchain and information security drives legal business by lowering trust costs, enabling smart contracts, and | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | | creating new practice areas (e.g., token regulation, DAO governance). | |
| | Topic 3.3. Doctrinal and legal approaches in determining the boundaries of regulation of blockchain technologies. | Doctrinal approaches range from strong regulation (treating blockchain as subject to all existing financial and data protection laws) to regulatory abstention (allowing "code as law" to govern). Legal approaches often focus on functional boundaries: distinguishing public blockchains (permissionless) from private ones (permissioned), and applying regulations based on use cases (e.g., payment tokens vs. utility tokens vs. security tokens). Key boundary issues include jurisdiction, data erasure (conflict with GDPR's "right to be forgotten"), and liability for smart contract execution errors. | LC,<br>S |
| | Topic 3.4. Foreign approaches to determine the boundaries of blockchain technologies regulation. | The European Union adopts a technology-neutral approach under the DLT Pilot Regime, allowing blockchain for financial market infrastructures while imposing robust AML/KYC obligations. The United States uses a fragmented model: the SEC treats certain crypto-tokens as securities, the CFTC classifies others as commodities, and state laws (e.g., Wyoming) enable DAOs as legal entities. Asia shows diverse approaches: Japan licenses crypto exchanges under the Payment Services Act, while Singapore provides a "sandbox" for blockchain innovation under its Monetary Authority. | LC,<br>S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | Topic 3.5. Technological solutions based on blockchain used in the field of public administration and legal activities. | Public administration applications include blockchain-based land registries (Georgia, Sweden), digital identity systems (Estonia's e-Residency), and transparent voting platforms (Sierra Leone). In legal activities, courts use blockchain for evidence timestamping (Chinese internet courts), lawyers employ smart contracts for automated escrow and royalty distribution, and notaries utilize blockchain for digital notarization of documents. These solutions improve transparency, reduce fraud, and streamline inter-agency data sharing. | LC, S |
| Requirements for information security with the use of blockchain technology. | Topic 4.1. Regulatory requirements for the technological, organizational and legal design of blockchain technology used for cryptography needs. | Technologically, blockchain used for cryptography must implement approved encryption algorithms (e.g., GOST 34.10-2018 in Russia) and secure key management practices. Organizationally, operators must establish access control policies, incident response procedures, and regular security audits, often certified under ISO/IEC 27001 or national equivalents. Legally, the design must comply with data localization laws, electronic signature regulations, and, for financial blockchains, central bank or financial authority licensing requirements. | LC, S |
| | Topic 4.2. The main problems of legal regulation of technologies based on the blockchain and analysis of law enforcement practice. | Key regulatory problems include the pseudonymity of blockchain transactions hindering AML compliance, the immutability conflicting with data correction rights, and the difficulty of determining | LC, S |

| Course module title | Course module contents (topics) | Topics contents | Academic activities types |
|---|---|---|---|
| | | liability for decentralized autonomous organizations (DAOs). Law enforcement practice shows courts struggling with smart contract interpretation, enforcement of cross-chain judgments, and seizure of crypto-assets stored on private keys. Additionally, inconsistent classification of tokens across jurisdictions creates legal uncertainty for blockchain-based businesses operating internationally. | |
| | Topic 4.3. The main problems of legal and information security of a person due to the introduction of blockchain technology in public relations. | Legal security problems include the irreversible loss of funds due to wallet key mismanagement, lack of effective consumer remedies for smart contract bugs, and the potential for blockchain surveillance to erode privacy (transparent ledgers). Information security issues involve side-channel attacks, 51% attacks on smaller chains, and phishing attacks targeting private key storage. Furthermore, the permanent storage of personal data on public blockchains may violate individuals' right to erasure under data protection laws, creating a fundamental tension between immutability and privacy. | LC, S |

* - filled in **only** **for full-time** education: LC - lectures; LW - laboratory work; S - seminars.

## 6. CLASSROOM EQUIPMENT AND TECHNOLOGY SUPPORT REQUIREMENTS

*Table 6.1. Classroom equipment and technology support requirements*

| Type of academic activities | Classroom equipment | Specialised educational / laboratory equipment, software, and materials for coursestudy (if necessary) |
|---|---|---|
| Lecture | A lecture hall for lecture-type classes, equipped with a set of specialised furniture; board (screen) and technical means of multimedia presentations. | A set of specialized furniture; technical means:<br>Monoblock<br>Multimedia projector<br>Screen for projector<br>Marker board<br>WiFi |
| Lab work | A classroom for laboratory work, individual consultations, current and mid-term assessment; equipped with a set of specialised furniture and machinery. | A set of specialized furniture; technical means:<br>Monoblock<br>Multimedia projector<br>Screen for projector<br>Marker board<br>WiFi |
| Seminar | A classroom for conducting seminars, group and individual consultations, current andmid-term assessment; equipped with a set of specialised furniture and technical means for multimedia presentations. | A set of specialized furniture; technical means:<br>Monoblock<br>Multimedia projector<br>Screen for projector<br>Marker board<br>WiFi, specialized software: Trados |
| Computer Lab | A classroom for conducting classes, group and individual consultations, current and mid-term assessment, equipped with personal computers (in the amount of 30 pcs), a board (screen) and technical means of multimedia presentations. | A set of specialized furniture; technical means:<br>Monoblock<br>Multimedia projector<br>Screen for projector<br>Marker board<br>WiFi |
| Self-studies | Aclassroom for independent work of students (can be used for seminars and consultations), equipped with a set of specialised furniture and computers with access to the electronic information and educational environment. | A set of specialized furniture; technical means:<br>Monoblock<br>Multimedia projector<br>Screen for projector<br>Marker board<br>WiFi |

* - It is necessary to specify a classroom for self-study of students

## 7. RESOURCES RECOMMENDED FOR COURSE STUDY

*Main readings:*


1. Vicente, D. M., & de Vasconcelos Casimiro, S. (Eds.). (2020). Data Protection in the Internet. Springer.
2. Walters, R., & Novak, M. (2021). Cyber Security, Artificial Intelligence, Data Protection & the Law. Springer.


*Additional readings:*


1. de Morais, C. B., Mendes, G. F., & Vesting, T. (Eds.). (2022). The Rule of Law in Cyberspace.
2. Albers, M., & Sarlet, I. (2022). Personality and Data Protection Rights on the Internet. Springer International Publishing.
3. Frenz W. (ed.). Handbook Industry 4.0: Law, Technology, Society. – Springer Nature, 2022.
4. Naef, T. (2023). Data Protection without Data Protectionism: The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law (p. 431). Springer Nature.


*Internet-(based) sources:*

1. Electronic libraries with access for RUDN students
- RUDN Electronic library system http://lib.rudn.ru/MegaPro/Web
- Electronic library system «University Library online» http://www.biblioclub.ru
- Electronic Library «URAIT» http://www.biblio-online.ru
- Electronic library system «Student. Consultant»www.studentlibrary.ru
- Electronic library system «Lan» http://e.lanbook.com/
- Electronic library system "Troitskyi most"

2. Databases and search engines:
- Electronic Legal and Regulatory Documentation Fund http://docs.cntd.ru/
- Search system Yandex https://www.yandex.ru/
- Search system Google https://www.google.ru/
- SCOPUS http://www.elsevierscience.ru/products/scopus/

*Training toolkit for self- studies to master the course *:*

* The training toolkit for self- studies to master the course is placed on the course page in the university telecommunication training and information system under the set procedure.

## 8. ASSESSMENT TOOLKIT AND GRADING SYSTEM* FOR EVALUATION OF STUDENTS' COMPETENCES LEVELUPON COURSECOMPLETION

The assessment toolkit and the grading system* to evaluate the competences formation level (competences in part) upon the course study completion are specified in the Appendix to the course syllabus.

* The assessment toolkit and the grading system are formed on the basis of the requirements of the relevant local normative act of RUDN University (regulations / order).

**DEVELOPERS:**

| Assistant Professor of Administrative and Financial Law Department | | A.R. Atabekov |
|---|---|---|
| Position, Name of the Department | Signature | Full name |

**HEAD OF THE DEPARTMENT**

| Head of Administrative and Finar Law Department, Full Professor | | O.A.Yastrebov |
|---|---|---|
| Position, Name of the Department | Signature | Full name |

**HEAD OF THE HIGHER EDUCATION PROGRAM**

| Head of Law Institute | | S.B. Zinkovskiy |
|---|---|---|
| Position, Name of the Department | Signature | Full name |