

DARS, d. d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 1/13
	Valid from:		

On 17 June 2021, the Management Board, pursuant to points 7. 2. 8, 7. 2. 10 and 12. 1 of the Articles of Association of DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI d.d., adopted the

Rules on the protection of business secrets

GENERAL PROVISIONS

Article 1 (Content)

These Rules set out the business secrets of DARS, d.d. (hereinafter: DARS or the Company), regulate the procedure for determining and designating business secrets, the protection of business secrets, the persons bound by the duty of business secrecy, and the obligations and responsibilities of these persons.

Article 2 (Protection of Business Secrets of other Economic Operators)

By applying the provisions of these Rules, mutatis mutandis, the protection shall also relate to business secrets of other companies, private entrepreneurs, economic interest groupings, foreign companies and their branches, which have been determined and designated as business secrets by these economic operators and forwarded to DARS.

DEFINITION, DETERMINATION AND DESIGNATION OF BUSINESS SECRETS

Article 3 (Business Secret)

- (1) The Company's business secrets cover undisclosed expertise, experience and business information that meet the requirements for business secrets in line with the Act governing business secrets.
- (2) In DARS, business secrets shall be protected at two levels and designated as a "BUSINESS SECRET" or "BUSINESS SECRET - CONFIDENTIAL" depending on the specific level of protection.
- (3) The "BUSINESS SECRET" shall in particular include the following information of DARS, the unauthorised acquisition, use or disclosure of which would harm the financial interests, strategic positions, competitive ability, technical potential or reputation of DARS:
 1. Business plans, financial plans, development plans and strategies;
 2. Risk management and internal control strategies;
 3. Internal and external audit reports;

DRAWN UP BY	REVIEWED BY	APPROVED BY
-------------	-------------	-------------

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 2/13
	Valid from:		

mag. Anton Travner	mag. Petar Škundrić	Management Board
--------------------	---------------------	------------------

4. Information on the Company's network, service and information systems and databases, as well as information included in the Company's databases, except for those expressly intended for the general public or users;
5. Software, computer applications and system products of the Company;
6. Information related to procedures in connection with reports on harassment;
7. Development and innovation projects;
8. Information on security areas, security risk assessments and security instructions, all related to the protection of classified information;
9. Information on security risk analyses and security plans, both related to the managed and information security system;
10. Information on business impact analyses and plans to ensure the integrity of the network and systems, both related to the business continuity management system;
11. Information on infrastructure risk assessments and infrastructure protection measures;
12. Information laid down as a business secret by regulations in the field of public procurement;
13. Information laid down as a business secret in line with internal acts;
14. Materials of the meetings of the Management Board, the Supervisory Board and the Supervisory Board committees.

- (4) "BUSINESS SECRET" also includes information determined as such by a decision of the Management Board, a Management Board advisor, manager of a division or another person, if so set out by another internal act of the Company. The Management Board may determine by decision that an individual document, which otherwise falls within the category of documents from the previous paragraph, is not a business secret.
- (5) The Management Board, Management Board advisor, a manager of a division, a head of internal auditing or another person may determine a higher level of protection by means of a decision on business secrecy if so set out by another internal act of the Company. The following in particular shall be designated with the higher level of protection "BUSINESS SECRET – CONFIDENTIAL":
- Information relating to internal investigations;
 - Information that, if disclosed to an unauthorised person, could make it difficult to carry out an impartial internal investigation, control or audit;
 - Other information for which it is assessed that unauthorised disclosure would have serious and irreversible consequences for the Company or financial consequences exceeding EUR 100,000.00.
- (6) All information that is or could be directly or indirectly related to the information from the previous paragraphs of this Article, in any material or electronic form (documents, audio and video media, computer floppy disks, CD-ROMs, hard disks, RAM, streamers, electronic mail, electronic memory, servers, mobile devices, photocopiers, fax machines, printers, and others) or in non-materialised form (any oral presentation of information, discussions about this information, and others) shall also be subject to professional secrecy.
- (7) Information shall be determined as a business secret upon its creation or at the start of the implementation of a business activity, the result of which is the information that has to be protected as a business secret.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 3/13
	Valid from:		

- (8) Information that is public by law, or information about a violation of the law or good business practices, cannot be determined as a business secret.

Article 4
(Decision Determining Business Secrets)

- (1) The decision determining business secrets referred to in the fourth and fifth paragraphs of Article 3 covers a description of possible serious adverse consequences for the interests of DARS, if the information was to be available to a person who is not entitled to become familiar with the business secret pursuant to these Rules, (hereinafter: unauthorised person), the term of validity or the method of termination of the protection of business secrets and user information. All persons who come into contact or become familiarised with the information designated as a business secret are to be informed of the decision.
- (2) The decision referred to in the previous paragraph of this Article is kept as an annex to the original document containing a business secret, or as an independent document, if the information determined as a business secret is located in a computerised database.

Article 5
(Designation)

- (1) All written documents and their duplications containing a business secret are to bear the words "BUSINESS SECRET" on at least the first page of the document, aligned with the right edge of the text of the document. Documents labelled with "BUSINESS SECRET – CONFIDENTIAL" must bear the label on each page of the document, and the Company's own documents must also be watermarked with "BUSINESS SECRET – CONFIDENTIAL" diagonally on each page. All other documents or media (maps, photos, CDs, DVDs, etc.) containing business secrets must be labelled "BUSINESS SECRET" or "BUSINESS SECRET – CONFIDENTIAL". If possible, the label "BUSINESS SECRET" or "BUSINESS SECRET – CONFIDENTIAL" should be written in bold letters larger than the letters of the text of the document. Each copy of the document is to be numbered with the sequence number of the copy.
- (2) If a document or medium is kept inside a case, this must be labelled to clearly indicate that it contains a business secret.
- (3) Each page of the document must also have a sequence page number indicated in the footer with regard to the total number of pages of the document.
- (4) A document containing a business secret may be sent to users in a closed non-transparent envelope by registered mail or by courier. The letter envelope sent by post must not be labelled "BUSINESS SECRET" or "BUSINESS SECRET – CONFIDENTIAL" or bear any other labels that would indicate the contents of the consignment. A consignment sent via a courier must be labelled "BUSINESS SECRET" or "BUSINESS SECRET – CONFIDENTIAL" and must be delivered directly to the user.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 4/13
	Valid from:		

- (5) When labelling the documents or media, information designated as a business secret must not be destroyed, damaged or rendered useless in any other way.
- (6) Documents labelled "BUSINESS SECRET – CONFIDENTIAL" may not be sent by e-mail or other remote communication devices, nor may they be copied, photographed or reproduced.

Article 6
(Cancellation of a Business Secret)

As a rule, the cancellation of the protection of information as a business secret, or the restriction of the internal use of information, is to be performed by the person who has determined the information as a business secret, or the Management Board.

Article 7
(In-house)

- (1) Information that does not comply with the conditions for being determined a business secret, but is intended for internal operations or use only by DARS employees due to its nature (for example: internal instructions, circulars to employees, draft documents that will be forwarded to clients or the public, etc.), may be labelled "IN-HOUSE".
- (2) The decision to label specific information as "IN-HOUSE" is to be adopted by the Management Board, the responsible person of the organisational unit, or the information is to be determined as such in the internal act.

ACCESS TO AND PROTECTION OF BUSINESS SECRETS

Article 8
(Users of Business Secrets)

- (1) Only DARS employees who need the information to perform their professional obligations and other individuals, who conclude a non-disclosure agreement with DARS that, as Annex 1, forms an integral part of these Rules or another agreement that corresponds in content to this agreement, or an information protection statement that, as Annex 2, is an integral part hereof, may become familiar with information that is a business secret.
- (2) The Management Board, Management Board advisors and managers of divisions, as well as DARS employees and other individuals who have been granted access to higher-level protected information by the Management Board, may get familiar with information designated as "BUSINESS SECRET – CONFIDENTIAL".
- (3) Pursuant to these Rules, DARS employees are considered to be individuals who are:
 - Employed based on an employment contract;

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 5/13
	Valid from:		

- Work at DARS based on an internship or scholarship contract;
 - Assigned to work in DARS as agency workers;
 - Perform professional obligations for DARS on another legal basis.
- (4) Access to business secrets must be limited in time and content to the extent absolutely necessary for the performance of a specific work or contractual obligation of the user.
- (5) Every document labelled "BUSINESS SECRET – CONFIDENTIAL" must include a list clearly showing who has taken note of the information, the reason to take note of the information, the exact time and date of taking note with the information, and the signature of the person who has taken note of the document.

Article 9

(Conditions for Granting Access According to the "BUSINESS SECRET – CONFIDENTIAL Protection Level")

- (1) Business secrets that are protected at the "BUSINESS SECRET – CONFIDENTIAL" level are available to the Management Board, the Management Board advisor and managers of divisions.
- (2) Moreover, the Management Board, the Management Board advisor and managers of divisions may grant access to business secrets protected at the "BUSINESS SECRET – CONFIDENTIAL" level to another employee, provided that:
- The employee has not been convicted of an offence of a corruptive, economic or property nature;
 - The employee is not the subject of ongoing criminal proceedings for offences referred to in the previous paragraph;
 - There are no security risks according to the person in charge of corporate security;
 - The employee is not in the process of the extraordinary termination of the employment contract or
 - The employment contract has not been suspended.
- (3) Access is granted for a period of five years. Following the end of that period, the employee who was granted access based on the second paragraph of this Article must apply for the granting of access to business secrets protected at the "BUSINESS SECRET – CONFIDENTIAL" level.
- (4) An employee who has been granted access based on the second paragraph of this Article must immediately inform the Management Board of the occurrence of circumstances due to which he/she no longer meets the conditions referred to in the second paragraph. Access to business secrets protected at a higher level shall cease to apply upon the occurrence of the circumstances referred to in the previous paragraphs or the termination of the employment contract.

Article 10

(Obligation to Protect Business Secrets)

- (1) The duty of professional secrecy shall occur at the time the user becomes familiar with it, and shall continue after the user ceases employment or function in DARS.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 6/13
	Valid from:		

- (2) Users are obliged to handle information determined and designated as a business secret in such a way that it is not accessible to unauthorised persons.
- (3) DARS employees shall confirm their commitment to the protection of DARS business secrets and awareness of the provisions of these Rules and other relevant regulations by signing the information protection statement, which, as Annex 3, is an integral part of these Rules; other users shall do so by signing the agreement or information protection statement referred to in Article 8 hereof.

Article 11

(Consent of the Management Board)

Employees may only publish articles, discussion papers and publications on issues or parts of issues set out as business secrets with the prior consent of the Management Board. The same applies to discussions at professional and scientific conferences.

Article 12

(Transmission of Business Secrets to State or European Authorities and Agencies)

- (1) The Management Board shall transmit business secrets to state or European authorities and agencies based on provided legal authorisation.
- (2) Entities referred to in the first paragraph shall only be provided with information that is necessary for the performance of their tasks.

Article 13

(Means of Protecting Business Secrets)

- (1) Documents protected at the "BUSINESS SECRET" level are kept to prevent access by unauthorised persons.
- (2) Business secrets protected at the "BUSINESS SECRET – CONFIDENTIAL" level are kept in burglary-resistant and fire-proof file cabinets with a lock or in a special room made available only to persons who are allowed to access this information. Every entry into the room is properly recorded; moreover, the room must be equipped with a video surveillance system and properly locked.
- (3) Documents labelled "BUSINESS SECRET – CONFIDENTIAL" are to be kept in the special records of the organisational unit.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 7/13
	Valid from:		

DAMAGE, CRIMINAL AND LABOUR LIABILITY

Article 14

(Damage and Criminal Liability)

- (1) A person who unduly, contrary to his/her duties regarding the protection of business secrets, communicates or presents information that is a business secret to a person, shall be liable to DARS for damages according to the regulations on damage liability and for a crime under the conditions stipulated by the Criminal Code.
- (2) If the damage cannot be precisely determined or the determination in this respect is associated with disproportionately high costs, a contractual penalty in the amount of EUR 5,000.00 shall apply for each individual breach by a DARS employee. The contractual penalty for the unauthorised disclosure of business secrets for persons not employed by DARS and for legal entities shall amount to EUR 20,000.00.

Article 15

(Employee Labour Liability)

- (1) An employee of DARS, who acts contrary to the provisions of these Rules, could commit a more serious violation of the obligations arising from the employment relationship.
- (2) Labour liability shall not exclude potential damage or criminal liability.

FINAL PROVISIONS

Article 16

(Final Provisions)

- (1) These Rules are to be published on the intranet.
- (2) With the entry into force of these Rules, the Rules on Determining and Protecting Business Secrets, applicable as of 27 July 2017, and the Instruction for Handling Information with Different Levels of Confidentiality, applicable as of 27 July 2017 shall cease to be valid.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 8/13
	Valid from:		

Annex 1: Non-Disclosure Agreement (Article 8 of the Rules)

THIS NON-DISCLOSURE AGREEMENT (“Agreement”) is hereby concluded on _____ by:

- 1) DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI D.D., Ulica XIV. divizije 4, 3000 Celje, Registration No. 5814251000, VAT ID No.: SI 92473717, represented by the Management Board (“**Beneficiary**”) and
- 2) _____ (name, surname / company)
address / registered office _____,
personal identification number (EMŠO) / registration no.: _____ (“**Person Liable**”).

(The Beneficiary and Person Liable are collectively referred to as the “**Parties**” and individually as the “**Party**”).

PRELIMINARY OBSERVATIONS

- (A) The subject of this Agreement is to define the content of collaboration between the Parties, which includes the exchange of confidential technical and business information, and the Parties agree that such information shall be kept confidential.
- (B) The Parties agree that the content of this Agreement is a business secret.
- (C) The Parties agree that this Agreement only forms a confidential relationship between them, without elements of any other business relationship.

IN LIGHT OF THE ABOVE and in consideration of the joint commitments and agreements specified herein, the Parties agree as follows:

Article 1

(Confidential Information)

- (1) For the purpose of this Agreement, the term “**Confidential Information**” means technical or business information provided in any form and manner (in oral, written, magnetic or optical form, materialized in the form of documents, software, promotional and presentation material, equipment and pilot projects) that is marked as confidential.
- (2) Confidential Information, provided in a written form, must be clearly marked with the label “BUSINESS SECRET” or “BUSINESS SECRET - CONFIDENTIAL” or any other phrase with a similar meaning.
- (3) Confidential Information, provided orally, must be shared with a warning about its confidential nature and the obligation to protect it under this Agreement.
- (4) Confidential Information is also considered to be information that is not explicitly marked as confidential or that is not marked with a label indicating the confidentiality of this information, but it is obvious that significant damage would occur if an unauthorized person found out about it or if the applicable legislation states that the disclosure or illegal management of data would violate applicable legislation.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 9/13
	Valid from:		

Article 2

(Exceptions from Confidential Information)

The following shall not be considered Confidential Information:

- 1) confidential information if the Person Liable can prove that it was known to them before the moment it was disclosed or shared by the Beneficiary under this Agreement;
- 2) information that was publicly available before the moment of disclosure or that became publicly known after, without any actions by the Person Liable that would constitute a breach of this Agreement;
- 3) confidential information if the Person Liable can prove that it was disclosed to them beforehand by another source, which does not originate from the Beneficiary, and that this source had the right to disclose such information;
- 4) confidential information for which the Person Liable was given a prior written consent by the Beneficiary;
- 5) information defined as public by law.

Article 3

(Protection of Confidential Information)

- (1) The Person Liable states that they shall treat any Confidential Information as a business secret, that they shall protect it with due diligence and that they shall ensure that those to whom this information may be provided or made known under this Agreement will adequately protect the information provided and will be informed about its confidential nature.
- (2) The Person Liable also states that they shall not disclose such information to any other third person or in any way provide it or make it available to the public, unless they acquire the written consent of the Beneficiary.
- (3) The Person Liable undertakes to prevent third parties, contractors or their employees making any use or disclosure of Confidential Information.
- (4) The Person Liable must immediately return all notes, documents in printed or electronic form or any other media that contain Confidential Information upon the Beneficiary's written request.

Article 4

(Permitted Disclosure and Distribution of Confidential Information)

- (1) The Person Liable shall only disclose any confidential information that is the subject of this Agreement in the original or a copy to those employees, contractors or third parties who need such information in order to achieve the purpose of this Agreement, and the Person Liable shall not in any way reproduce or otherwise distribute any item or document that is Confidential Information by nature or contains, in whole or in part, Confidential Information without the prior written consent of the Beneficiary.
- (2) If the Person Liable discloses confidential information referred to in the previous paragraph, they are obliged to conclude written non-disclosure agreements with the persons to whom the Beneficiary's Confidential Information is disclosed, which ensure the protection of the Confidential Information at least to the extent that it is protected by this Agreement.
- (3) The Person Liable shall immediately notify the Beneficiary if the Person Liable is obligated to disclose any Confidential Information, provided by the Beneficiary, so that the Beneficiary may exercise all applicable legal remedies to protect the Confidential Information. The Person Liable undertakes to

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 10/13
	Valid from:		

collaborate with the Beneficiary in exercising lawful legal remedies or in any other action to protect the Confidential Information that the Beneficiary may request.

Article 5

(Breach of the Non-Disclosure of Confidential Information Obligation)

- (1) The Person Liable is aware that a breach of the provisions of this Agreement would amount to irreparable damage to the Beneficiary. In the event of a breach, the Beneficiary has the right to seek judicial protection, with which they demand from the Person liable the immediate cessation of potential or actual breaches of this Agreement.
- (2) The Beneficiary and the Person Liable agree that in the event of a breach of provisions from this Agreement, the Person Liable shall be obligated to pay for all actual damages that occurred and lost profit. If the damage could not be precisely determined or if the determination of it would be associated with disproportionately high costs, a contractual penalty in the amount of EUR 20,000.00 applies, namely for each individual breach of obligations by the Person Liable. The payment of the contractual penalty is due within seven days from the day the Person Liable receives the Beneficiary's claim for the payment of the contractual penalty via registered mail.

Article 6

(Rights related to Confidential Information)

- (1) All Confidential Information provided by the Beneficiary to the Person Liable, either in full or in part, shall remain the property of the Beneficiary.
- (2) All rights related to the Confidential Information, which is the subject of this Agreement, remain exclusively with the Beneficiary.
- (3) No provision in this Agreement shall constitute permission, copyright or the granting of rights of use or license and other rights to the Person Liable with regard to or on the basis of information.
- (4) The Person Liable undertakes that they shall not dispute ownership or any other right over the Beneficiary's Confidential Information.

Article 7

(Personal Data)

In accordance with the act, governing the protection of personal data, the Beneficiary permits the processing of personal data for the purpose of establishing and keeping records and the performance of contractual rights and obligations under this Agreement.

Article 8

(Final Provisions)

- (1) All disputes and claims, arising from or in relation to this Agreement, are settled by the court with the competent jurisdiction in Ljubljana.
- (2) This Agreement is concluded and enters into force as of the date it is signed.
- (3) The Agreement shall remain in force until the Beneficiary terminates the obligation of the Person Liable to protect the confidential information in writing, or until the Parties agree to that in writing, or until the Confidential Information stops being a business secret and becomes publicly known and accessible.
- (4) If any provision of this Agreement is or becomes wholly or partially invalid, unenforceable or ineffective, the validity of the other provisions shall not be affected.

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 11/13
	Valid from:		

(5) This Agreement may only be amended through a written arrangement made by both Parties.

Beneficiary

Person Liable:

DARS, D. D.

In _____, on _____

In _____, on _____

(signature)

(signature)

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 12/13
	Valid from:		

Annex 2: Information Protection Statement (Article 8 of the Rules)

Name and Surname:
Company name:
Address:
Postcode and post:

I undertake that I shall do everything necessary to protect the information obtained during the contractual cooperation with DARS. I shall not sell, trade, publish or provide information to unauthorized employees and external parties and shall not disclose it in any way without the prior written consent of the person responsible at DARS. I shall use the information solely for the contractual purpose and shall consider it unconditionally confidential for an unlimited time.

I also undertake that, in accordance with the Personal Data Protection Act, I shall not use any personal data that I come across during the performance of the contractual obligations and also before the conclusion of the Agreement, contrary to the provisions of this Act and the Agreement. I shall not use personal data for any other purpose other than the purposes that are or will be defined in the Agreement, even if the Agreement is terminated or after it ends.

I shall ensure conditions and measures for the protection and safeguarding of personal data to prevent its possible misuse, alteration or loss, accidental or intentional unauthorized destruction and unauthorized processing within the meaning of the provisions of the said Act and contractual requirements set out by DARS.

In the event of any damage suffered by DARS due to the violation of the prohibition on the disclosure of information and personal data in accordance with this statement, contractual provisions and legislation in the Republic of Slovenia, DARS may exercise moral, indemnification and criminal liability against the signatory of this statement. If the damage could not be precisely determined or if the determination of it would be associated with disproportionately high costs, a contractual penalty in the amount of EUR 20,000.00 applies, namely for each individual breach by the Person Liable.

(Place and date of statement signing)

(Signature)

DARS d.d.	IN-HOUSE		
Rules on the protection of business secrets	Version:	1	Page: 13/13
	Valid from:		

Annex 3: Information Protection Statement (Article 10 of the Rules)

Pursuant to Article 10 of the Rules on the protection of business secrets

(Name and surname, date of birth, address) hereby

DECLARE

that I am familiar with the Articles of Association of DRUŽBA ZA AVTOCESTE V REPUBLIKI SLOVENIJI d.d. and the Rules on the Protection of Business Secrets.

By signing this statement, I expressly acknowledge that I understand and accept it as a confidentiality agreement; moreover, I undertake to refrain from any action that, given the nature of the work I perform at DARS, materially or morally harms or could harm the reputation and business interests of DARS and to act in line with the provisions of the internal acts, and to implement measures to protect business secrets, personal data and company assets within the scope of my responsibilities and powers.

I am aware that a violation of the Rules on the Protection of Business Secrets may constitute a more serious violation of the obligations arising from the employment relationship.

(Place and date of statement signing)

(Signature)

To be kept at:

- SUK, Human resources folder