

# RUŽIČKA CSEKES

ADVOKÁTSKA KANCELÁRIA



Are you ready for inspection by  
the Office for Personal  
Data Protection?



2018  
Domáca  
advokátska kancelária



2017  
Domáca  
advokátska kancelária



2016  
Domáca  
advokátska kancelária



2015  
Domáca  
advokátska kancelária



2014  
Domáca  
advokátska kancelária



2013  
Domáca  
advokátska kancelária

## Are you ready for inspection by the Office for Personal Data Protection?

The preparation for the implementation of the GDPR has been challenging and the date of entry into force on 25. May 2018 surprised many businesses. We are bringing you the opportunity to check, whether you are or will be prepared, if your company is inspected by the Office for the Personal Data Protection of the Slovak Republic (hereinafter only as the “Office”).

### When can the Office come to inspect?

1. If a personal data breach occurs;
2. At the request of a data subject, who claims to be directly concerned in his/her rights;
3. Even without a notified breach, but on the basis of routine inspection activity of the Office, according to its plan of inspections;
4. If you initiate proceedings before the Office in connection with consultations concerning your new product or service and these are to affect personal data, in such case the Office can also conduct an inspection.

In any of these cases, you need to be prepared. Sanctions associated with the GDPR can reach astronomical sums. So what does it mean to be prepared for an inspection by the Office?

### What specifically do you need to meet and how do you demonstrate fulfilment of this obligation?

Obligation under the GDPR	Content	Documents that need to be submitted <sup>1</sup> x/✓
<b>Meeting obligations under Art. 5 (2) and Art. 24</b>	Demonstration of appropriate technical and organizational measures adopted by the company.	<ul style="list-style-type: none"> <li><input type="checkbox"/> Privacy notice, privacy terms, most often in the form of Information memo for internal and external purposes (mostly on the Intranet or the web).</li> <li><input type="checkbox"/> Consents and records on them.</li> <li><input type="checkbox"/> Procedures for exercising the rights of data subjects.</li> <li><input type="checkbox"/> Procedures in case of privacy breach.</li> <li><input type="checkbox"/> Procedures for informing data subjects and the Office in case of a privacy breach.</li> <li><input type="checkbox"/> Recording of the processing contracts by the processor or sub-processor.</li> </ul>

<sup>1</sup> For illustrative purposes we used the title of the document that we encounter most often. However, the content of the document that has to meet the criteria of GDPR requirements, is essential.

		<ul style="list-style-type: none"> <li>□ Procedures for transferring data to the third countries (including binding internal rules).</li> <li>□ Contractual documentation in connection with the processing/use of personal data with the confidentiality obligation (labour law, B2B).</li> <li>□ Instructions and regular trainings for authorized persons processing personal data under the supervision of the controller or the processor.</li> <li>□ Procedures for monitoring internal and external entities at the controller's premises.</li> <li>□ Appointment of the data protection office as well as communicating of contact details and appointment to the Office.</li> <li>□ Regular review of policy and measures to ensure compliance with the Personal Data Protection Act and the GDPR.</li> <li>□ Assessment of correctness of original consents with personal data processing (in some cases, the consent is obtained from the data subject, while the processing takes place under another legitimate purpose).</li> </ul>
<p><b>Records of processing activities</b></p>	<p>Each controller and processor are required, under Art. 30, to keep records. The Office published on its website a template of the record, please check whether your record conforms with the template available by the Office.</p>	<ul style="list-style-type: none"> <li>□ Record on processing activities and their update.</li> </ul>
<p><b>Data protection impact assessment (DPIA)</b></p>	<p>If your company processes data that can lead to a high risk for personal data protection, the controller will perform impact assessment on data protection. The GDPR in Art. 35 (3) expressly defines 3 cases, when the processing may lead to a high risk and such assessment is necessary, but this may not be a final number. First of all, it is necessary to carry out the data protection impact assessment for any processing operation that may lead to the risk and also the Office is entitled</p>	<ul style="list-style-type: none"> <li>□ DPIA- Risk analysis for the processing of personal data and their mitigation through measures</li> <li>□ Prior consultations with the Office and compliance with the measures imposed by the Office.</li> <li>□ Procedure to ensure reassessment in case of occurrence of events foreseen by the law.</li> </ul>

	<p>to issue a list of further processing operations for which the assessment will be required. The Office is required by the GDPR to consult the process of developing such assessment.</p>	
<p><b>Specifically designed and standard personal data protection</b></p>	<p>When placing new product or service on the market, as mentioned above, when a data protection impact assessment is not necessary, it is possible to develop a similar document. Developing such documentation may be simpler than a data protection impact assessment and if necessary, it can become a great tool to demonstrate your readiness for personal data protection in a given product or service.</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Privacy by design and default.</li> <li><input type="checkbox"/> DPIA – Risk analysis for the personal data processing and their mitigation via measures.</li> <li><input type="checkbox"/> Set up the highest standard of personal data protection from the start of the project.</li> </ul>
<p><b>A legitimate interest as a reason for lawful processing</b></p>	<p>Administrative analysis of legitimate interest, from which all conditions for personal data processing are derived, including retention periods.</p> <p>Where the legal basis for data processing is identified as the legitimate interest of the controller, it is necessary to take into account the following 4 criteria:</p> <ul style="list-style-type: none"> <li>• Proper identification of legitimate interest</li> <li>• Demonstration that processing is necessary to achieve the purpose</li> <li>• Assessment, whether the rights and freedoms of the person concerned do not outweigh such interest</li> <li>• Limiting personal data to only what is necessary – the minimization principle</li> </ul> <p>Subsequent fulfilment of information obligations.</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Legal analysis of processing operations.</li> <li><input type="checkbox"/> Minimizing the use of consents as the legitimate purpose for the processing of personal data between parties with unequal status (employee and employer).</li> </ul>

The ability to demonstrate to the Office compliance with the GDPR provisions is a key element in the personal data protection. Your company should be able to demonstrate it to the Office at least in the extent of the documentation that will contain the above mentioned recommended attributes.

The Office also issues as a guide, document entitled: “30 Steps to Compliance with the New Legislation on Privacy Policy”, however, it should be noted that this document is not a manual, but only a summary of the main requirements of the GDPR and the Personal Data Protection Act.

## Should you have any questions, do not hesitate to contact us:



**JUDr. Lucie Schweizer**  
lucie.schweizer@r-c.sk



**JUDr. Darina Parobeková, LL. M.**  
darina.parobekova@r-c.sk

*The Compliance area, which includes also GDPR, is perceived in the world as an essential part of operation of each successful company. In Ružička Csekés Law Firm we are dealing with these issues practically from its beginnings. Our Compliance team provides advice in the field of legal risk assessment in connection with KYC, KYE processes, IT security including cyber security, personal data processing, including GDPR, business secret document management and human resources issues.*

# Ružička Csekés s.r.o.

Information pursuant to Act no. 136/2010 Coll.  
Limited Liability Company founded in line with Slovak law.

Seat:

Vysoká 2/B, 811 06 Bratislava, Slovak Republic

Tel: +421 (0)2/32 33 34 44

Fax: +421 (0)2/32 33 34 43

Email: [office-ba@r-c.sk](mailto:office-ba@r-c.sk)

IČ DPH: SK2022827620

Entered in the Commercial Register of District Court Bratislava I, Section Sro, Entry no. 58431/B, Id. no. (IČO): 36 863 360.

Entered in Slovak Bar Association (hereinafter as "SAK") on 04 June 2009.

Authorization to provide legal services and legal consulting (attorney services) in line with Act no. 586/2003 Coll. on Advocacy as amended, established based on registration of the company in the register kept by SAK having its seat at Kolárska 4, 813 42 Bratislava, Slovak Republic.

The company provides attorney services in compliance with the provisions of Act no. 586/2003 Coll. as amended and in line with relevant SAK regulations based on client agreements governed by Slovak law. In case of service provision to foreign entities, Slovak court competent based on the seat of the company pursuant to Slovak legal regulations has jurisdiction.

Liability for damage caused by company in provision of legal services is regulated by Act no. 586/2003 Coll.

Company's liability is subject to insurance taken out with the insurer Starr International (Europe) Ltd., registered address: 30 Frenchchurch Avenue, London, EC3M 5AD, United Kingdom, registration number: 09654797, represented on the basis of a power of attorney by: Starr Underwriting Agents Limited, registered address: 30 Frenchchurch Avenue, London, EC3M 5AD, United Kingdom, acting in the Slovak Republic through its organizational branch Starr Underwriting Agents Limited Slovakia, organizačná zložka, Panenská 5, 811 03 Bratislava, Slovak Republic. Insured risks: provision of legal and professional services, Policy no.: 7707024613. Insurance cover: 15,000,000 EUR for any one and all insurance claims during the insurance term.

The company provides services for a fee, the amount and form of which are to be agreed contractually before commencing the provision of services in line with the Decree of Ministry of Justice SR no. 655/2004 Coll. as amended.

Grievances or complaints regarding the services provided by the company may be submitted at company premises.

Other information about the company may be obtained at company offices.