

Your World First

C/M/S/

Law . Tax

To-Do list of tasks for compliance with data protection for operators of smart buildings and those providing or using similar services

December 2019

Contacts



Dóra Petrányi

CEE Managing Director
T +36 1 483 4820
E dora.petranyi@cms-cmno.com



Gábor Czike

Partner
T +36 1 483 4819
E gabor.czike@cms-cmno.com



József Várady

Partner
T +36 1 483 4840
E jozsef.varady@cms-cmno.com



Márton Domokos

Senior Counsel
T +36 1 483 4824
E marton.domokos@cms-cmno.com

This task list summarises the data protection (GDPR) compliance related documents and tasks to be done by operators of smart office buildings, and the persons obtaining or providing smart office services. Naturally, all data protection and compliance projects and all data processing organisations are unique. Thus not all the steps below will be relevant for operators or service providers of office buildings or organisations that obtain these services, who will need to adhere to other or different steps.

	Task / Documents needed for compliance	Details	Who or what prescribes it? What are the takeaways from the regulatory practice?
General tasks / documentation needed for data compliance			
	Internal records of data processing operations	<p>An internal record of the data processing operations of the operator (e.g. processing of partner contacts, employees, visitors, etc.).</p> <p>In order to ease administrative tasks, the responsibilities of individuals should be divided into groups. (e.g. partners, contact persons, employees, visitors, etc.)</p>	<p>Mandatory under Article 30 of the GDPR.</p> <p>In general, compliance of internal records of data processing operations is verified by the Hungarian National Authority for Data Protection and Freedom of Information ("NAIH") for comprehensive, extensive larger-scale investigations. Usually, when records are not complete, the authority may find other violations of law as well.</p>
	Preparing a Data Protection Notice	<p>Information on personal data processing operations including:</p> <ol style="list-style-type: none"> processing the personal data of contact persons of sub-contractors (cleaning staff, security staff, property manager, IT service providers); processing the personal data of contact persons of tenants or operators, and processing the data of visitors receiving entry cards into the building (e.g. card numbers) and other data associated with these visitors (e.g. using cafeteria services); circulars sent to lessees 	<p>Mandatory under Articles 13-14 of the GDPR</p> <p>In one case, the Austrian data protection authority set a fine of EUR 55,000 on a healthcare service provider among others for the incomplete information provided to the individuals, while in another case the NAIH fined a financial services provider EUR 3,030 for not providing information about the processing of a telephone number and other violations.</p>

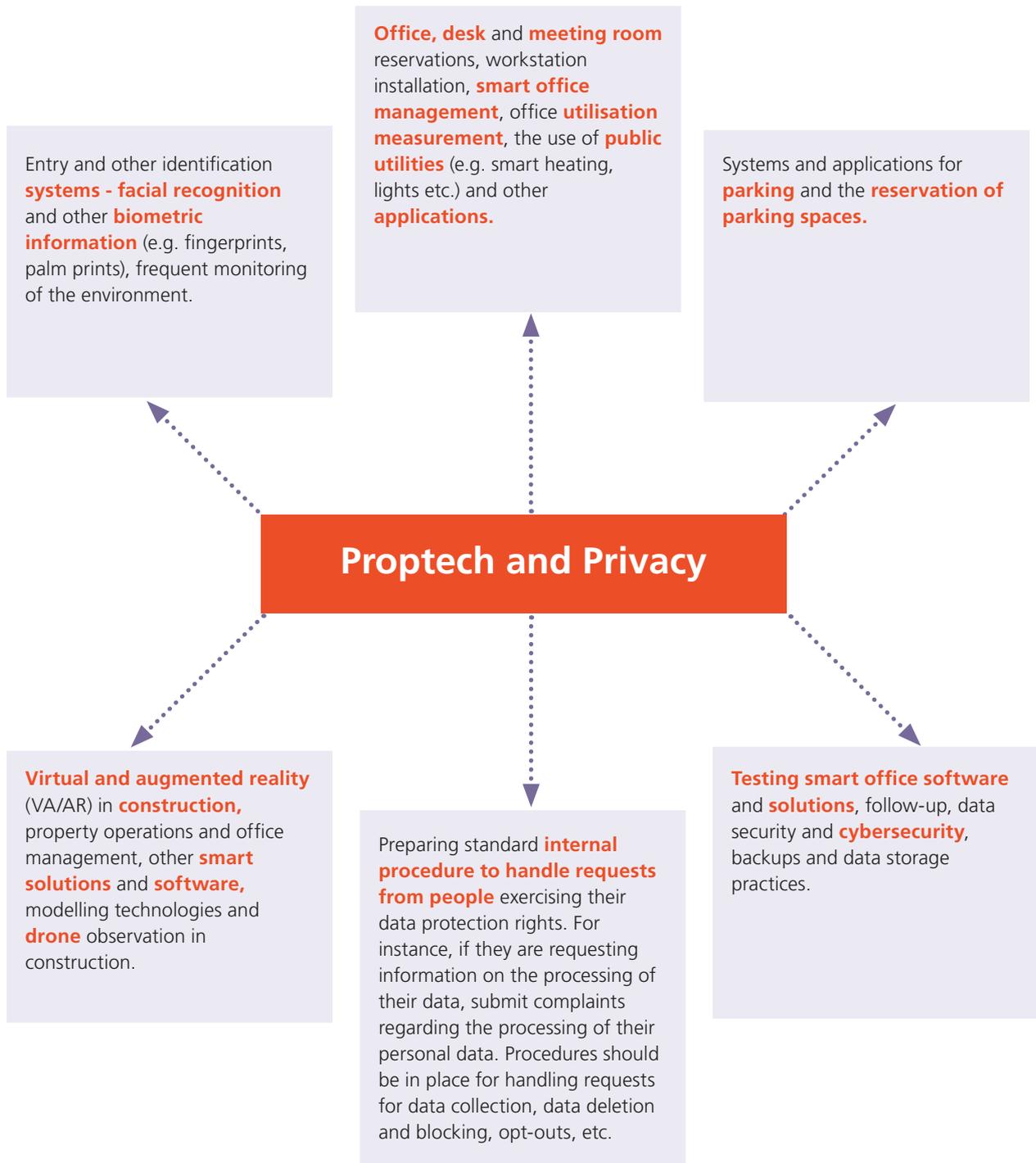
	<p>Preparation of data protection consent forms – if the processing of the personal data of visitors, sub-contractors, lessors and other individuals require their consent</p>	<p>Consent may be obtained through either electronic or paper-based forms, and wording and disclosure may vary according to the nature of the data processing.</p>	<p>Mandatory under Article 7 of the GDPR.</p> <p>The Greek data protection authority imposed a data protection fine of EUR 150 on a consultancy firm that asked for consent to process the data of employees in an unlawful manner. Although the employees volunteered consent, the company should have designated another legal basis for the processing.</p>
	<p>Implementing and documenting so-called “legitimate interest tests” expected under GDPR – if the personal data of visitors, sub-contractors, lessees and other individuals is not processed or their data is not based on their consent, the fulfilment of a contract concluded with them (as natural persons) or on the fulfilment of legal obligations, but is based on the “legitimate interest” of the operator.</p>	<p>The legitimate interest test provides details about the circumstances of personal data processing for the individuals. Data processing based on “legitimate interest” refers to a security camera system or the use of an electronic entry system.</p>	<p>Mandatory under Article 6 Section 1 (f) of the GDPR.</p> <p>NAIH imposed a data protection fine of EUR 90,909 for the unlawful processing of personal data of festival-goers. In this case, the authority also reviewed the legitimate interest test drafted by the company and found it unlawful in several respects.</p>
	<p>Reviewing data security measures and related consultancy</p>	<p>The operator must introduce organisational and technical measures that guarantee the security of data, and to adjust all measures to its operation. This refers to measures for the management of and access to various IT systems, internal regulations, and individual measures applying to software or data processing operations (e.g. firewalls, anti-virus software, access management, etc.).</p>	<p>Mandatory under Article 32 of the GDPR.</p> <p>Following a comprehensive review, the UK data protection authority imposed a fine of more than EUR 115,010,000 on an international hotel chain for a personal data breach that affected the IT system of one of the chain’s companies and for implementing insufficient data protection measures.</p> <p>In another case, the French data protection authority imposed a fine of EUR 400,000 on a property services company for insufficient data security and a deficiency with data storage.</p>

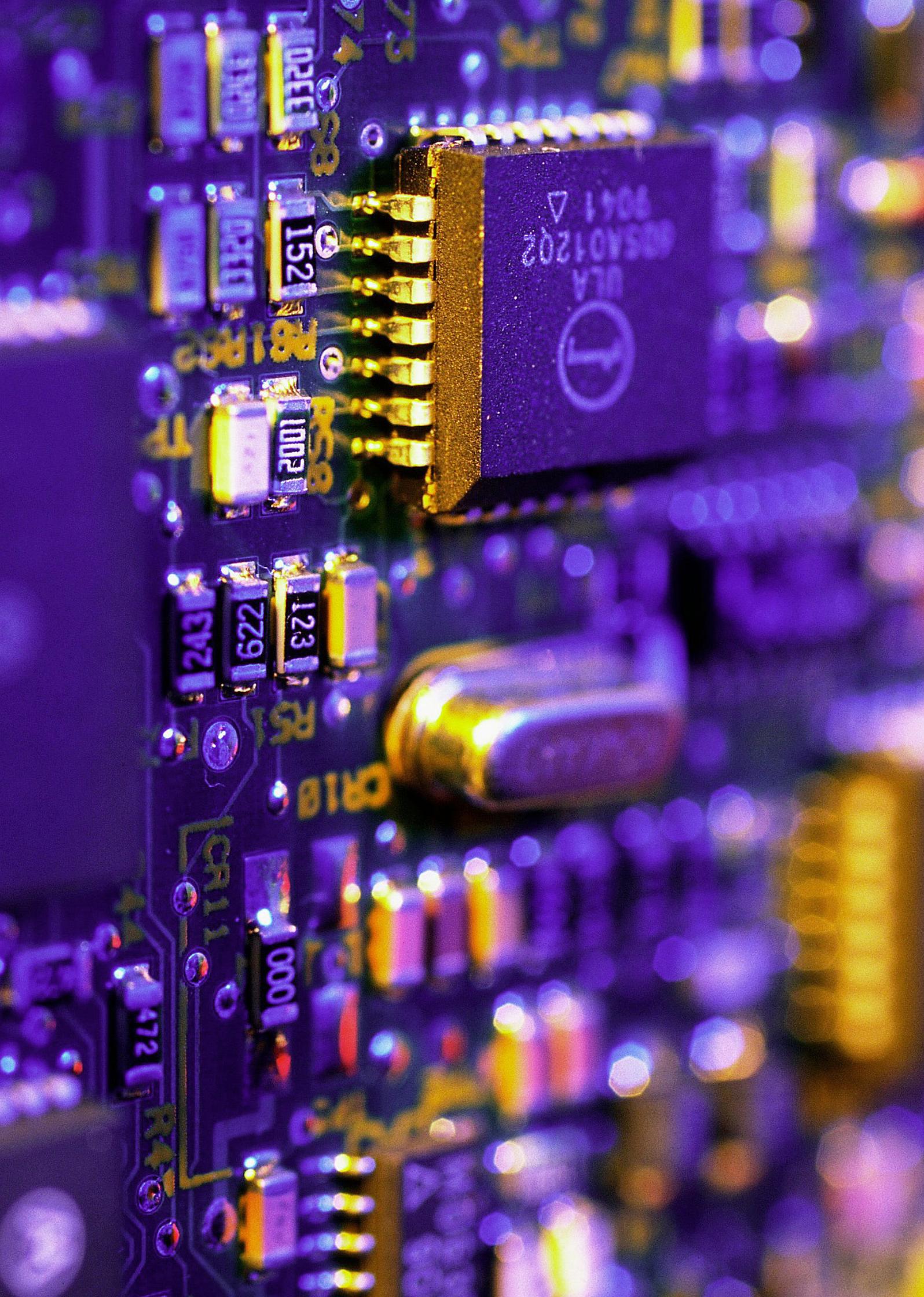
	<p>Preparing internal personal data breach management procedures and the related internal document templates.</p>	<p>In cases of hacker attacks or the abuse of biometric data (i.e. data theft) affecting the database of the lessee or a contracting partner, this breach must be reported to the data protection authority and, depending on the degree and nature of the incident, the relevant individuals must also be informed (e.g. by email or in a local-media communique). Related breach management documentation will provide effective assistance to the people involved.</p>	<p>Mandatory under Articles 33-34 of the GDPR.</p> <p>NAIH imposed a data protection fine of EUR 33,333 on a social organisation for insufficient breach management and for gaps in data security after a hacker attack on its database.</p>
	<p>Reviewing the operator's data transfer practice (both within and outside the corporate group)</p>	<p>Signing "data processing agreements" with persons/ organisations processing personal data on behalf of the operator, preparing a template data processing agreement, and proposing the procedural order for the conclusion and follow-up of similar contracts.</p> <p>The other commercial contracts signed with data processors (who are processing personal data on behalf of operators, such as IT service partners) and with data controllers (e.g. banks and/or insurance providers who act according to their own professional rules regarding individual decision-making rights) must also be reviewed: in particular, those provisions on confidentiality, B2B marketing, contacts and communications, and the use of references.</p> <p>In the case of data transfers to non-EU member states, separate measures are necessary. Usually, this requires signing an additional contract, such as the EU data transfer model contract (with the EC Model Clause / Standard Contractual Clause).</p>	<p>Mandatory under Articles 44-50 of the GDPR.</p> <p>NAIH imposed a data protection fine of EUR 3,030 after the unlawful transfer of personal data, which was revealed by whistle blowers.</p>

	<p>Preparation of data protection impact assessments and internal guidelines to assess when it is necessary to carry out a data protection impact assessment, the steps necessary for it, and when consultations should be held with the relevant people and/or the competent authority</p>	<p>Carrying out and documenting a Data Protection Impact Assessment (DPIA) is mandatory in certain high-risk cases such as the application of new technologies, processing the data of children, biometric data processing, etc. The mandatory cases in which DPIA are necessary were published by all EU member states. In Hungary, a blacklist can be accessed on the website of NAIH (National Authority for Data Protection and Freedom of Information): https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf</p> <p>A DPIA is typically required in cases of smart offices, biometric data identification systems, the profiling of individuals (e.g. analyses of their behaviour), the processing of location data and smart metering.</p>	<p>Mandatory under Articles 35-36 of the GDPR.</p> <p>We expect that authorities will verify DPIAs more often in the future.</p>
	<p>Preparing a warning sign (with pictograms), a data protection notice and internal operational rules for security cameras.</p>	<p>The GDPR provides greater freedom for companies to determine the purpose of CCTV recordings and how long the recordings should be kept. However, increased emphasis needs to be applied for individuals to exercise their data protection rights. Therefore, it is advisable to hold data protection training more frequently and set out an internal procedure to manage data inquiries and requests.</p>	<p>In line with the GDPR and the applicable laws on asset protection.</p> <p>In one case, the NAIH imposed a EUR 3,030 fine on a company for the inappropriate management of an individual's data protection access request, including not providing a copy and restricting the processing of the recording).</p>

	<p>Guard Service Guidelines and the review of the entry process, as well as the use of the entry system from a data protection point of view.</p>	<p>Companies must prepare the relevant data protection related documents with a view to the specific nature of guard services and the entry process. This includes information regarding entry or asset protection measures and internal data protection regulation. It is advisable to hold compliance training for the staff in charge.</p>	<p>Necessary under Article 5 (2) of the GDPR (<i>principle of accountability</i>).</p> <p>The NAIH ascertained events organised by a Hungarian festival organising company may have led to unlawful data processing. The NAIH ruled that data processing was carried out under an inappropriate legal basis, with the violation of the principles of purpose limitation and data minimisation. It ultimately imposed a fine of EUR 90,909 on the company.</p>
	<p>Reviewing data processing for HR purposes</p>	<p>An office building operator and any company providing or using smart office services must plan their data processing according to its HR organisation's strategy. This includes preparing a data protection notice for employees or leased employee and, reviewing internal HR policies.</p> <p>We recommend preparing a separate data protection notice for job applicants. Contractual relations with head-hunters, job-mediating portals and manpower leasing firms also need to be re-examined.</p>	<p>Necessary under Article 5 (2) of the GDPR (<i>principle of accountability</i>), and under Articles 13 and 14 of the GDPR.</p> <p>The NAIH imposed an EUR 3,030 fine on an organisation who unlawfully disclosed the personal data of a whistleblower following the detection and reporting of a non-compliance at the workplace.</p> <p>In addition, the NAIH established the liability of a public administration organisation in connection with a data protection non-compliance, because its director has unlawfully received the personal data of whistleblowers who submitted a report regarding such director.</p>

	<p>Reviewing the data processing operations related to the website of the building operator, reviewing website terms and conditions and cookie information</p>	<p>The documentation of data processing must be prepared according to the characteristics of a given website (i.e. the use of cookies, services via the site, etc.).</p>	<p>Mandatory under Articles 13-14 of the GDPR.</p> <p>A German data protection authority imposed a EUR 20,000 fine on a social media provider for insufficient data security measures and for leaking user data on their website.</p>
	<p>Review of the data company's marketing and client relation activities and programmes</p>	<p>Data protection notices, consent templates and data transfers are of key importance in this area. Note that this could apply to the data protection notices and consent forms pertaining to ad campaigns and prize awards. Information for programmes should be stated according to the characteristics of a given event.</p>	<p>Mandatory under Articles 6, 13 and 14 of the GDPR.</p> <p>The French data protection authority imposed a EUR 50,000 data protection fine on a company for, among other things, failing to obtain the voluntary and informed consent of the individuals for individualised advertisements, and for unlawful marketing activities.</p>
	<p>An internal proceeding for visitors and other individuals to exercise their data protection rights.</p>	<p>This includes requests for information on processing personal data, complaints against processing, requests for rectification, requests for erasure or blocking the data processing, opt-outs, etc.</p>	<p>Required under Chapter III of the GDPR.</p>
	<p>Compliance training materials</p>	<p>Educational materials and training sessions should be prepared according to the requirements of each employee and sub-contractor group. Test questions may also be included in educational materials.</p> <p>Compliance training and educational materials can also be provided for employees of the office building and, if needed, their sub-contractors.</p>	<p>Necessary under Article 5 (2) of the GDPR (<i>principle of accountability</i>).</p>





9041
605A01202



U1A

152

1002

123

229

10001

CR11

472



Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices.

CMS locations:

Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

cms.law

1911-0113204