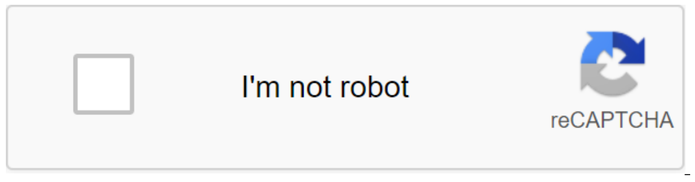
Gdpr pdf eur lex



Continue

Data protection rules as a trust in the EU and beyondIn general Data Protection Regulation1 (further regulations) have been applied throughout the European Union for more than a year. It is at the heart of the EU's consistent and modernized data protection landscape, which also includes the Data Protection Directive2 and the Data Protection Regulation for EU agencies and bodies3. This framework should be completed under the Electronic Privacy Regulation, which is currently in the legislative process. Strict data protection rules are necessary to ensure the fundamental right to protect personal data. They are central to a democratic society4 and an important component of an increasingly data-driven economy. The EU seeks to take advantage of the many opportunities that digital transformation offers in terms of services, jobs and innovation, while at the same time addressing the challenges they bring. Identity theft, data breaches, discrimination against individuals, built-in bias, sharing illegal content, and developing intrusive surveillance tools are just a few examples of issues that are increasingly highlighted in public debate, where it is clear that people expect their data to be protected. Data protection has become a truly global phenomenon as people around the world increasingly value and value the protection and security of their data. Many countries have adopted or are in the process of adopting comprehensive data protection rules based on principles similar to the principles of the Regulation, leading to a global convergence of data protection rules. This opens up new opportunities to facilitate data flows between commercial operators or government agencies while increasing the level of personal data protection in the EU and around the world.1 Regulation (EU) 2016/679 of the European Parliament and The Council of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and the free movement of such data, and the repeal of Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1): Directive (EU) 2016/680 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with respect to the processing of personal data by the competent authorities in order to prevent, investigate, detect or prosecute criminal offences or the execution of criminal penalties, as well as the free movement of such data , as well as the cancellation of the Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016: . The directive must be rescheduled by Member States by May 6, 2018. Security Union reports ensure the state of play on its transposition.3 Regulation (EU) 2018/1725 and the Council of 23 October 2018 on the protection of persons non-processed personal data by The Union's institutions, authorities, agencies and agencies, as well as the free movement of such data, as well as the repeal of Regulation (EC) No. 45/2001 and Decisions No. 1247/2002/EC, OJ L 295, 21.11.2018, page 39-98: . It was applied on 11 December 2018.4 by the Supreme Court of India in a landmark decision of 24 August 2017, recognizing confidentiality as a fundamental right, a significant aspect of human dignity.2Data protection is taken more seriously than ever before and it has a broad impact on various stakeholders and sectors. The Commission is determined to lead the EU to the successful implementation of the new data protection regime and to support all aspects of it that will be fully operational. Through this Message, the Commission will take stock of the progress achieved so far in the consistent implementation of data protection rules throughout the EU, the functioning of the new governance system, the impact on citizens and businesses and the EU's efforts to promote global convergence of data protection regimes. It reports to the Commission on the application of the Regulation of January 20185 and it was informed of the work of the Group of 6, in particular its contribution to annual training, as well as discussions held at the preparation event organized by the Commission on 13 June 20197. This report is also a contribution to the review that the Commission plans to undertake by May 2020. It is becoming part of the regulatory framework for expanding policy spectrum including health and research, artificial intelligence, transportation, energy, competition and law enforcement. The Commission has consistently stressed the importance of properly implementing and enforcing the new data protection rules, as outlined in the January 2018 Regulation and its Personal Data Use Guide in the context of the September 2018 elections. At the time of this communication, significant progress has been made towards this goal, although the situation certainly needs to be fully addressed. One continent, one law: Member States have a data protection framework One of the key objectives of the Regulation was to understand the fragmented structure of the 28 different national laws that existed under the previous Data Protection Directive10, and to provide legal certainty for individuals and entities throughout the EU. This goal has been largely achieved.5 Commission to the European Parliament and the Council strong protection, new opportunities - Guidance of the Commission on the direct application of the General Data Protection Regulation as of May 25, 2018, COM (2018) 43 finals: Multi-party Regulatory Group, created by the Commission, includes representatives of civil society and business, academics and practitioners: Article 97 Of Regulation.9 'Guide to the Commission on the Application of the Union Data Protection Act in the Context of Elections', COM (COM) 2018) 638 Final: Https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf.10 Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals in relation to the processing of personal data and the free movement of such data harmonization of the legal frameworkHost Regulation directly applicable in Member States , it obliges them to take a number of legal steps at the national level, in particular to create and distribute powers to national data protection authorities11, to establish rules on specific issues, such as harmonizing the protection of personal data with freedom of expression and information, and amending or repealing sectoral laws with aspects of data protection. At the time of this communication, all but three Member States have updated their national data protection law. Work to adapt industry laws continues at the national level. Following its inclusion in the European Economic Area Agreement, the application of the Regulation was extended to Norway, Iceland and Liechtenstein, which also enacted their national data protection law. However, stakeholders are calling for even greater harmonization in some areas.13 Indeed, this provision allows Member States to further specify their application in some areas, such as the age at which children consent to online services14 or the processing of personal data in areas such as medicine and health. In this case, the actions of Member States are framed by two elements: (i) any national specification law must comply with the requirements of the Charter of Fundamental Rights15 (and not go beyond the framework established by the Charter);ii) it cannot infringe on the free flow of personal data within the EU16. In some cases, Member States have introduced national requirements at the top of the Regulation, particularly in many sectoral laws, resulting in fragmentation and Burden. One example of the additional requirement imposed by Member States at the top of the Regulation is the obligation under German law to appoint a data protection officer in companies with 20 employees or more constantly involved in the automated processing of personal data. Continuing its efforts to better harmonize the Commission is engaged in a bilateral dialogue with national authorities, where it focuses on national measures: effective independence of data protection bodies, including through adequate financial, human and technical resources; as national laws restrict the rights of data subjects;11 Such as the right to impose administrative fines.12 As of July 23, 2019, Greece, Portugal and Slovenia are still in the process of enacting their national law.13 Report by the Many Stakeholders Group on Regulations of 13 June 2019: 13 years for Belgium, Denmark, Estonia, Finland, Latvia, Malta, Sweden and the United Kingdom; 14 years for Austria, Bulgaria, Cyprus, Spain, Italy and Lithuania; 15 years for the Czech Republic and France; 16 years for Germany, Hungary, Croatia, Ireland, Luxembourg, the Netherlands, Poland, Romania and Slovakia.15 Article 8.16 Under Article 16 (2) of the Treaty on the Functioning of the European Union.4 the fact that national legislation should not impose requirements beyond the Regulations when there is no framework for specification, such as additional conditions for processing; fulfilling the obligation to harmonize the right to protect personal data with freedom of expression and information, taking into account that this obligation should not be misused to create a frightening impact on journalistic work. The work of data protection bodies cooperating in the context of the European Council for Data Protection (Council) is a key factor in the consistent application of the new rules: enforcement measures affecting a number of Member States go through a mechanism of cooperation and coherence within the Council, and the guidelines adopted by the Council contribute to a coherent understanding of the Regulation. Nevertheless, stakeholders believe that data protection authorities will go further in this direction. The work of the national courts and the Court of Justice of the European Union also contributes to a consistent interpretation of data protection rules. National courts have recently ruled to invalidate the provisions of national laws that come out of Regulation 18.III All parts of the new system of government fall into force Regulatory has created a new governance structure, putting at the center of the center of independent national data protection bodies as bodies Regulation and the first contact points for stakeholders. While most data protection authorities benefited last year from increased resources, there are still large differences among Member States.19 Data protection bodies are using their new powers Regulation to give data protection authorities with stronger enforcement powers. Contrary to concerns raised by some stakeholders prior to May 2018, national data protection authorities have adopted a balanced approach to enforcement. They focused on dialogue rather than sanctions, especially for the smallest operators, who do not process personal data as their main activity. At the same time, they have not shied away from effectively using their new powers when necessary, including through social media investigations20 and administrative fines of between several thousand euros and several million, depending on the severity of data protection violations.17 Article 60 of the Regulation provides for cooperation between data protection authorities to apply a single interpretation of the Regulation in specific cases. Article 64 provides that in some cases the Council will issue opinions in order to ensure that the Regulation is applied consistently. Finally, the board has the power to make binding decisions to data protection authorities in the event of a disagreement between them.18 This was the case in Germany and Spain19 for example, the Irish Data Protection Commission has opened 15 official investigations into compliance with the Multinational Technology Company Regulation. See page 49 of the Irish Commission for Data Protection's 2018 annual report: 5S00 fines imposed by data protection authorities: 5,000 euros on a sports betting cafe in Austria for illegal video surveillance; 220,000 euros at a data brokerage company in Poland for not informing individuals that their data is being processed; 250,000 euros imposed on the Spanish football league LaLiga for lack of transparency in the development of its smartphone app; 50 million euros on Google in France, due to the conditions for obtaining consent from users. In conducting investigations, it is important that data protection authorities collect relevant evidence, comply with all procedural steps in accordance with national law and ensure due process in often complex files. This takes time and includes a considerable amount of work, which explains why most investigations initiated after the enactment of the Regulation are still ongoing. At the same time, the success of the Regulations measured not by the number of fines imposed, but by changes in the culture and behaviour of all actors. in context, data protection authorities have other tools at their disposal, such as imposing a temporary or final processing restriction, including a ban or order to suspend data flows to a recipient in a third country.22 Some data protection agencies have created new tools, such as help lines and tools for businesses, while others have developed new approaches, such as regulatory sandboxes23 to assist companies in their compliance efforts. However, a number of stakeholders continue to feel that they have not received sufficient support and information, in particular small and medium-sized enterprises in some Member States.24 To help remedy this situation, the Commission provides grants to data protection authorities for them to reach out to stakeholders, in particular individuals and small and medium size enterprises25. Several of the decisions imposing fines are still subject to judicial review.22 Article 58(2)(f) and (j).23 See report of the Multi-stakeholder Group on GDPR: EUR 2 million allocated to nine data protection authorities in 2018 for activities in 2018-2019: Belgium, Bulgaria, Denmark, Hungary, Lithuania, Latvia, the Netherlands, Slovenia and Iceland: 1 million euros will be allocated in 2019: the European Data Protection Council is working Data Protection Guardians have stepped up their work in the European Council for Data Protection26. This intensive work has enabled the Council to adopt some 20 guidelines on key aspects of Regulation27. The future direction of the Council's work is presented in the two-year programme28, as required by cross-border affairs Regulation.In, each data protection body is no longer just a national body, but is part of a truly entire ES process at all stages, from investigation to decision-making. Such close cooperation has become a daily practice: by the end of June 2019, 516 cross-border cases had been initiated through the cooperation mechanism. The Commission actively contributes to the work of the Council29 to promote the letter and spirit of the Regulation and recalls the general principles of EU legislation30. The new management system still needs to be fully implemented in order to create a culture of EU data protection. It is important that the Council improve the adoption process and develop eu EU general data culture among its members. The ability of data protection authorities to join forces on issues affecting more than one Member State, such as joint investigations and coercive measures, can help achieve this goal while mitigating limited resources. Many stakeholders would like to see more cooperation and a unified approach on the part of national data protection authorities.32 They also ask for greater consistency in the recommendations provided by data protection authorities and full alignment of national guidelines with the Council's guidelines. Some are also awaiting further clarification of key concepts of the Regulation, such as the risk approach, taking into account, in particular, the problems of small and medium-sized enterprises. In this context, it is essential that stakeholders be given the opportunity to make better use of the Council's work. That is why the Commission welcomes the systematic public consultations organized by the Guidelines Board. This practice, together with the organization of stakeholder seminars26, the Council has a legal personality and consists of the heads of the national data protection oversight bodies and the European Data Protection Comptroller.27 As a non-voting party.30 The Commission has also helped to smooth the establishment of the Council and supports its functioning by providing its communications system.31 Article 62 Regulation.32 See. The Report of the Regulatory Interest Group: enterprises believe that national lists of types of processing operations that require an assessment of the impact on data protection under Article 35 of the Regulation could be better agreed.33 Including between different federal government.7on targeted topics at an early stage of reflection, should be continued and strengthened to ensure transparency, Individuals enjoy their rights, but awareness must continue while the basic purpose of the Regulation is to strengthen the rights of individuals. More awareness of data protection rightsIndividuals in the EU are increasingly aware of data protection rules and their rights: 67% of respondents in May 2019 Eurobarometer34 know about the Rule and 57% know that there is a national data protection body to which can seek information or file a complaint. 73% have at least one of the rights granted by the Regulation. However, a significant number of people in the EU still do not take active measures to protect their personal data when they go online. For example, 44% of people have not changed their default privacy settings on social networks. Individuals are increasingly exercising their rights. Businesses also report that in a number of sectors, such as banking and telecommunications, the number of requests for access to personal data has increased. In addition, individuals are increasingly withdrawing their consent and exercising their right to object to commercial communications.36 However, some operators have reported misunderstandings of individuals regarding data protection rules, such as the belief that individuals must consent to all processing or that the right to be removed is absolute (while, for example, personal data must sometimes be stored by operators due to legal obligations).37 For their part, civil society organizations have complained of long delays in responses from some business and data protection authorities. It is important to note that non-governmental organizations have begun to take a number of representative measures after they have been authorized by individuals, using the new opportunity under Regulation 38. It would be easier to call for representative action if more Member States took advantage of the opportunity to allow non-governmental organizations to take action without a mandate39.34 See the report of the Data Protection Unit with many stakeholders under the General Data Protection Regulation.37 The Group's report in accordance with the General Data Protection Regulation.38 Article 80 (1) Regulation.39 Article 80 (2) Regulation.8 The need to continue efforts to raise awareness of the Dialogue and public outreach efforts should thus continue at the national and EU level. To that end, in July 201940, the Commission launched a new online campaign to encourage people to read privacy statements and optimize their privacy settings. Businesses generally welcome the principle of accountability of the Regulation, which departs from the previous onerous ex ante (removal of notification requirements, scalability of obligations and flexibility of data protection by design and default, allowing competition based on privacy-friendly solutions). decisions). at the same time, some are calling for greater legal certainty and additional or clearer guidelines from data protection authorities.41 Sound Data Management Companies report a number of challenges in adapting to the new rules, many stressing that it was also an opportunity to bring data protection to the attention of the company's boards, put their home in order in terms of the data they hold, improve security, be better prepared for incidents, reduce the impact of unnecessary risks and build more trusting relationships with their customers and commercial partners. As for transparency, business organizations and civil society organizations point to a delicate balance between providing individuals with all the information they need in accordance with the Regulation, and using clear and simple expressions and forms that people can understand. Operators are developing innovative solutions in this direction. In general, companies have indicated that they have been able to implement the new rights of the data subject, although it is sometimes difficult to meet deadlines because of the increase in the number of requests and their wider nature43, or to verify the identity of the person, making a request.40 This follows a previous campaign to distribute information materials to individuals and entities available on the following issues: See. The Executive Group's report on Regulation.42 The it system update is often cited as one of the main problems Particularly with regard to the implementation of data protection principles by design and default, the right to erase in back-ups, etc. 43 Enterprises also advocate guidelines from the Council on unreasonable and excessive requests.9Impact on innovationRegulation not only allows, but also encourages the development of new technologies while respecting the fundamental right to protect personal data. So this can be done in areas such as artificial intelligence. Businesses have begun to develop their offers of new, more confidential services. For example, search engines that do not track users and do not use behavioral advertising are

gradually gaining market share in some Member States. Other companies are developing services that rely on new rights granted to individuals, such as the portability of their personal data. A growing number of businesses have promoted respect for personal data as a competitive edifator and point of sale. These developments are not limited to the EU, but also concern very innovative foreign economies.44 The specific situation of micro- and small-scale enterprises is low-risk, although the situation varies between Member States, micro- and businesses that did not process personal data because their core business was among the with most questions about the application of the Regulation. While they appear to be due in part to a lack of awareness of data protection rules, their concerns are sometimes compounded by campaigns by consultants seeking paid advice, the dissemination of false information, such as the need for systematic consent from individuals, and additional requirements at the national level. In this context, micro- and small-scale enterprises are calling for the development of guidelines that are tailored to their particular situation and that provide very practical information. Some data protection authorities have already done so at the national level.47 In addition to national initiatives, the Commission has published information materials to help such companies comply with the new rules through a series of practical steps.48 The use of the toolkit under the Regulation provides tools for demonstrating compliance, such as standard contractual provisions, codes of conduct and recently introduced certification mechanisms. Standard contractual provisions are the type of provisions that can be included on a voluntary basis in a contract, such as between a data controller and a data processor, and which lay down the obligations of the contractual parties under the Regulation. For example, according to a report published by the Israeli Cybersecurity Industry Association, in 2018, the cybersecurity sub-sector Data Protection and Privacy was the fastest growing sub-sector as a result of partial entry into the use of GDPR.45 As defined in the definition of SMEs, By telephone: Regulation, in fact, does not rely only on consent, but provides several legal grounds for processing personal data.47 For example, a guide developed by the French data protection authority: use standard contractual provisions for both international transfers and within the EU49. As far as international translations are concerned, their widespread use shows that they are very useful to enterprises in their enforcement efforts and are particularly beneficial to companies that do not have the resources to enter into individual contracts with each of their data contractors. A number of sectors also consider the adoption of standard treaty provisions as a useful way to promote harmonization, particularly when adopted by the Commission. The Commission will work with parties to take advantage of the provisions and update existing provisions. Compliance with codes of conduct another operational and practical tool used by industry to help demonstrate compliance with Regulation 51. These codes should be developed by trade associations or regulators representing the categories of controllers and processors, and should describe how data protection rules can be implemented in a particular sector. Calibrating risk-taking obligations can also prove to be a very useful and cost-effective way for small and medium-sized enterprises to meet their obligations. Finally, certification can also be a useful tool to demonstrate compliance with specific Regulations. This can increase legal certainty for business and promote regulation around the world. The certification and accreditation guidelines recently adopted by the European Data Protection Council will allow the development of CERTIFICATION schemes in the EU. The Commission will monitor these developments and, if necessary, use the authority granted under the Regulation to develop certification requirements. The Commission may also issue a standardization request to EU standards authorities on items relating to Regulation.VI. Ascending convergence is progressing internationallyInsesses on the protection of personal data are not limited to the EU. As a recent global survey on internet security has shown, trust deficits are widening around the world, forcing people to change the way they behave online.54 An increasing number of companies 49 See Article 28 of the Regulations. The standard contractual provisions adopted by the Commission take advantage of all European reality. In contrast, those that have been adopted under Article 28 (8) by the data protection authority, bind only to the body that has adopted them and thus can be used as standard contractual provisions for processing operations that fall under the jurisdiction of that body, under Articles 55 and 56.50 They are in fact the main tool on which companies rely to export their data.51 The European Data Protection Board adopted guidelines on codes of conduct on 4 June 2019. They clarify procedures and rules related to the submission, approval and publication of codes both at the national and EU level.52 Concert 98 Regulation.53 See. 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. According to the survey, 78 per cent of those surveyed were concerned about their online privacy, with 49 per cent saying their distrust had caused them to disclose less personal Online, while 43% said they care more about keeping their devices safe.11 rights created by the Regulation for their non-EU clients. In addition, as countries around the world increasingly face similar challenges, they are equipping themselves with new data protection rules or upgrading existing ones. These laws often have a number of commonalities that are shared by the EU data protection regime, such as comprehensive legislation rather than sectoral rules, the rights of individuals to be enforced and an independent oversight body. This trend is truly global, it goes from Korea to Brazil, from Chile to Thailand, from India to Indonesia. Another clear sign of this upward convergence trend is the increasingly universal membership of the Council of Europe's Convention 108'55, recently modernized56 with significant contribution from the Commission. Promoting safe and free data flows through decisions on adequacy and beyond this evolving convergence opens up new opportunities for facilitating data flows and therefore trade, as well as cooperation between government agencies, while increasing the level of protection of individuals' data in the EU when they are transferred abroad. In implementing the strategy outlined in the 2017 report on the exchange and protection of personal data in a globalized world57, the Commission has stepped up cooperation with third countries and other international partners, building on further evolving elements of convergence between privacy systems. This included exploring the possibility of drawing conclusions on adequacy with individual third countries.58 This work has yielded important results, in particular the entry into force in February 2019 of the EU-Japan Mutual Adequacy Agreement, which has created the world's largest area of free and secure data flows. Negotiations on adequacy with the South Korean side are at an advanced stage, and research is under way to begin negotiations on adequacy with a number of Latin American countries, such as Chile or Brazil, depending on the completion of the current legislative processes. Events are also promising in some parts of Asia, such as India, Indonesia and Taiwan, and in theand 39% responded that they use the Internet more selectively, among other precautions. The survey was conducted in 25 countries: Australia, Brazil, Canada, China, Egypt, France, Germany, United Kingdom, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russia, Republic of Korea, Sweden, Tunisia, Turkey and the Council of Europe Convention of 28 January 1981 on the protection of individuals regarding the automatic processing of personal data (ETS No. 108) and the 2001 Supplemental Protocol on the Protection of Individuals supervisory authorities and cross-border data flows (ETS No. 181). is the only binding multilateral document for data protection. The latter countries that have ratified the Convention include Argentina, Mexico, Cape Verde and Morocco.56 The Protocol on Amendments to the Convention on the Protection of Individuals on The Automatic Processing of Personal Data (ETS No. 108), agreed at the 128th session of the Committee of Ministers in Elsinore, Denmark, 17-18 May 2018. The summary text of the modernized Convention 108 is available on the Commission's report to the European Parliament and the Council Sharing and Protecting Personal Data in a Globalized World, COM/2017/07 final.58 The Regulation also created an opportunity for conclusions on adequacy also for international organizations as part of EU efforts to facilitate the exchange of data with such entities.12European Eastern and Southern Areas that could open doors for future decisions. At the same time, the Commission welcomes the fact that other countries that have put in place transfer instruments similar to the adequacy of the Regulation have recognized that the EU, as well as countries recognized by the EU as adequate, provide the necessary level of protection.59 This could lead to the creation of a network of countries where data is free to flow. At the same time, intensive work is under way with other third countries, such as Canada, New ealand, Argentina and Israel, to ensure continuity in accordance with the Adequacy Decision Regulation adopted under the 1995 Data Protection Directive. Meanwhile, the EU-US Privacy Shield has proven to be a useful tool for providing transatlantic data flows based on a high level of protection, with more than 4,700 participating companies.60 Its annual review ensures that the system is functioning regularly and that new issues can be resolved on time. Since there is no one-size-fits-all solution for data flows, the Commission is also working with stakeholders and the Council as a full-capacity Regulatory toolkit for international translations. This applies to instruments such as standard contractual provisions, the development of certification schemes, codes of conduct or administrative arrangements for public bodies. In this regard, the Commission is interested in sharing experience and best practices with other systems that may have developed special expertise in some of these tools. The Commission will consider the use of the powers granted under the Regulation on these transfer instruments, especially standard contractual provisions. In addition to purely bilateral instruments, it could also be explored whether like-minded countries can create a multinational framework in this area at a time when data flows are becoming an increasingly important component of trade, social interactions. Such a document would allow data to flow freely between treaty parties, while providing the necessary level of protection based on shared values and converged systems. It could be developed, for example, through the modernized Convention 108 or draw inspiration from the Free Data Flows initiative launched by Japan earlier this year. By developing new synergies between trade and data protection tools, helping to bring data protection standards closer together at the international level, the Commission is also committed to combating digital protectionism. To that end, it had developed specific provisions on data flows and data protection in trade agreements it systematically implemented in its bilateral and multilateral negotiations, such as the current WTO e-commerce negotiations. These horizontal provisions exclude purely protectionist measures, such as coercive requirements for data localization, While maintaining the regulatory autonomy of the parties to protect the fundamental right to data protection.59 This is an approach adopted, for example, by Argentina, Colombia, Israel and Switzerland.60 This means that in the first three years of its existence, Privacy Shield has more participating companies that its predecessor, Safe Harbor, was after 13 years of operation.13Gde dialogues on data protection and trade negotiations should go separate ways. , they can complement each other: the agreement on mutual adequacy between the EU and Japan is the best example of such synergies, further weakening trade exchanges and thereby strengthening the benefits of the Economic Partnership Agreement. In fact, this kind of convergence, based on shared values and high standards and backed up by effective enforcement, provides the strongest basis for the exchange of personal data, which is increasingly recognized by our international partners.61 Given that companies are increasingly operating across borders and opting to apply similar rules in all their business operations around the world, this convergence contributes to creating an environment conducive to direct investment, facilitating trade and building confidence among commercial partners. Promoting information-sharing to combat crime and terrorism through appropriate safeguards can also make it much easier to share information between the EU and foreign regulators, police and the judiciary, and thereby facilitate better and faster law enforcement cooperation.62 To that end, the Commission is considering decisions on adequacy in accordance with the Data Protection Directive to enhance cooperation with key partners in the fight against crime and terrorism. Also about the umbrella63 between the EU and the United States, which forces in February 2017, can be used as a model for similar agreements with other important security partners. Other examples pointing to the importance of high data protection standards as a basis for stable law enforcement cooperation with third countries include the transfer of passenger name records (PNR)64 and the exchange of operational information between Europol and important international partners. In this regard, the negotiations on international agreements are reflected, for example, in reference to the concept of Free Flow of Data with Confidence in the Osaka Leaders' Declaration G20: The Commission's communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee for the Security of Regions of com (2015) 185 final.63 the EU-US Agreement on the Protection of Personal Data when it is transferred and processed to prevent, Investigation, detection or prosecution of criminal offences, including terrorism, within the framework of police cooperation and judicial cooperation in criminal cases: (01) (Umbrella Agreement). The Umbrella Agreement is the first bilateral international law enforcement agreement to provide a comprehensive catalogue of data protection rights and responsibilities under EU agreements. This is a successful example of how law enforcement cooperation with an important international partner can be strengthened through negotiations on a strong set of data protection safeguards.64 United Nations Security Council Resolution 2396 of 21 December 2017 calls on all UN member states to develop the capacity to collect, process and analyse PPR data, with full respect for human rights and fundamental freedoms. See also The Message from the Commission's European Security Agenda, COM (2015)185 Final: current or ready to start with several countries in the southern neighborhood65.Strong data protection guarantees will also be an important component of any future agreement on cross-border access to electronic evidence in criminal investigations, bilateral (EU-US agreement) or multilateral level (Second Additional Protocol to the Council of Europe Convention on Cybercrime)66.Promoting cooperation between data protection authorities While privacy issues or security incidents can affect a large number of individuals simultaneously in several jurisdictions, closer forms of cooperation between oversight bodies at the international level can help ensure both effective protection of individual rights and more stable conditions for business operators. Against this backdrop, and in close contact with the Council, the Commission will work on ways to promote cooperation in law enforcement and mutual assistance between EU bodies and foreign oversight bodies, including through the use of new powers under Regulation 67. This could cover various forms of cooperation, from the development of common interpretive or practical tools to the exchange of information on ongoing investigations. Finally, the Commission also intends to intensify its dialogue with regional organizations and networks, such as the Association of Southeast Asian Nations (ASEAN), the African Union, the Asia-Pacific Privacy Forum (APPA) or the Ibera-American Data Protection Network, which are playing an increasingly important role in shaping common data protection standards, facilitating the exchange of best practices and strengthening law enforcement cooperation. It will also work with the Organisation for Economic Co-operation and Development and the Asia-Pacific Economic Cooperation to bring the data protection together. VII. Data protection legislation as an integral part of a wide range of personal data protection policies is guaranteed and integrated into a number of policies of the Union of Telecommunications and Electronic Communications Services The Commission adopted its proposal to regulate privacy and electronic communications in January 201769. The proposal is aimed at protecting the confidentiality of communications, as stipulated in the Charter of Fundamental Rights, as well as to protect 65 see article 50 of the International Data Protection Act. This provision covers a wide range of forms of cooperation, from information on data protection legislation to complaints and investigative assistance.68 Such as general templates for breach notifications.69 data that may be part of the message, as well as terminal equipment of end users. The proposed ePrivacy Regulation complements and complements the Regulation by establishing specific rules for the aforementioned purposes. It is modernizing the existing e-privacy rules to take account of technological and legal changes. It enhances the privacy of individuals by extending the scope of the new rules to include also more leading telecommunications providers, thereby creating a level playing field for all electronic communication. While the European Parliament passed a mandate to launch trilogs in October 2017, has not yet agreed on a common approach. The Commission remains fully committed to the E-Commerce Regulation and will support co-legislators in their efforts to quickly adopt the proposed Regulation. These include providing medical care or treatment, protecting against serious cross-border health threats, and ensuring high standards of quality and safety of health care, as well as medicines or medical products. The provision establishes rules that ensure that health and data are processed and shared throughout the EU. These rules also apply to third-party access to patients' medical data, including data that are held in patient resumes, ePrescriptions, and, in the long term, comprehensive electronic medical records, and their use for scientific research purposes. In a specific area of clinical trial, the Commission has also prepared specific questions and responses to the interaction between the Clinical Trials Regulation71 and the General Data Protection Regulation72.Artificial Intelligence ('AI') As AI becomes strategically important, it is important to shape the global rules for its development and use. By promoting the development and development of AI, the Commission has chosen a human-centred approach, which means that applications for AI must be in line with basic rights.73 In this context, the rules set out in the Regulation provide a common framework and contain the 70This Directive of the European Parliament and the Council of 12 July 2002 regarding the processing of personal data and the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive) OJ L 201, 31.7.2002, page 37-47.71 The Commission's Announcement of 8 April 2019 on the creation of trust in human-oriented artificial intelligence: Https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.Ethics Guidelines for Reliable AI presented by the High Level Expert Group (HLEG) on 8 April 2019: . See also the OECD Council on Artificial Intelligence Recommendation: G20 Principles Approved under the G20 Osaka Leaders Declaration: and the statement of the G20 ministers on trade and the digital economy: the economy: obligations and rights that are particularly relevant for the processing of personal data in AI. For example, the Regulation provides for the right not to be subjected to exclusively automated decision-making, except in certain situations.74 It also includes specific requirements for transparency in the use of automated solutions, namely the obligation to inform and provide meaningful information and to explain its relevance and the implications of processing for individuals.75 These basic principles of the Regulation have been recognized by the High Level Expert Group on AI76, the Organization for Economic Cooperation and Development77 and G2078 as particularly relevant to addressing problems and emerging issues. The European Data Protection Council has identified AI as one of the possible topics in its work programme for 2019-202079. TransportThe development of connected cars and smart cities is increasingly dependent on the processing and exchange of large amounts of personal data between several parties, including cars, car manufacturers, telematics service providers and government agencies responsible for road infrastructure. This multi-party environment has some difficulties in the distribution of roles and responsibilities of the various actors involved in the processing of personal data and how to ensure the legality of processing by all actors. Compliance with ePrivacy Regulations and Laws are essential to the successful deployment of intelligent transport systems across all modes of transport and the proliferation of digital tools and services to ensure greater mobility for individuals and products.80 EnergyThe development of digital solutions in the energy sector is increasingly dependent on the processing of personal data. The Clean Energy for All Europeans package includes new provisions allowing electricity to be digitized and data access, data management and data compatibility rules that allow real-time processing of consumer data to achieve savings and encourage self-anxiety and participation in the energy market. Compliance with data protection rules is therefore essential for the successful implementation of these provisions.74 Article 22 Regulation.75 Article 13(2) (f) Regulations.76 Recommendation of the Artificial Intelligence Council: Statement of G20 Ministers on Trade and Digital Economy: For example, by promoting planning and use of various vehicles throughout their journey.81 In particular, the Electricity Directive: of personal data is increasingly becoming an element to be taken into account in competitive politics82. Given that data protection authorities are the only authorities charged with assessing data protection breaches, competition, consumer protection and data protection authorities cooperate and will continue to cooperate if their respective competencies need to be crossed. The Commission will strengthen such cooperation and closely monitor developments. Electoral contextIn its Guide to the Use of Personal Data in the Context of Elections83, issued in September 2018 as part of the Electoral Package84, the Commission drew attention to rules of particular importance to polling subjects, including issues related to micro-targeted voters. This guidance was reflected in the European Data Protection Council Statement85, and a number of data protection authorities have issued guidance at the national level. The electoral package also included a call for each Member State to establish a national electoral network with national electoral authorities with competence in election matters and those responsible for monitoring and enforcing rules, such as data protection, on online election-related activities. New measures have also been introduced to impose sanctions for breaches of data protection rules by European political parties and foundations. The Commission recommended that Member States adopt the same approach at the national level. Data protection aspects will also be taken into account when assessing the 2019 European Parliament elections, due to be published in October 2019. Law enforcement agencies can only be built on full respect for the fundamental rights enshrined in the EU Charter and EU secondary law, including appropriate data protection safeguards to ensure the safe exchange of personal data for law enforcement purposes. Any restrictions on the fundamental right to privacy and data protection are subject to strict need and proportionality test.82 For example, the case M.8788 - Apple / Shazam and the case of M. M.8124 - Microsoft / LinkedIn.83 . Conclusion Based on the information available to date and the dialogue with the Commission's preliminary assessment by the parties was that the first year of application was generally positive. However, as shown in this further progress is needed in a number of areas. Implementation and complementary legal framework: Three Member States that have not yet updated their national data protection law are doing so urgently. All Member States must finalize their sectoral legislation to the requirements of the Regulation. Ensuring that the new governance system fully realizes its potential: Member States must allocate sufficient human, financial and technical resources to national data protection authorities. Member States should facilitate such investigations. It should continue its work on the guidelines, especially for small and medium-sized enterprises. interaction between data protection authorities and other authorities, particularly from the competition, in full respect to their respective competencies. Support and engagement: The Council needs to expand the way stakeholders are involved. The Commission will continue to provide financial support to data protection authorities to help them reach stakeholders.19 The Commission will continue its efforts to raise awareness and work with stakeholders. Promoting international convergence: The Commission will continue to intensify its dialogue on adequacy with key partners, including in the field of law enforcement. In particular, it intends to conclude ongoing negotiations with the South Korean side in the coming months. In 2020, the commission will report a review of 11 adequacy decisions made under the Data Protection Directive. and a facilitator of cooperation (e.g. the Free Flow of Data with Trust initiative launched by Japan in the context of the Group of 20). Regulations require the Commission to report on its implementation in 2020. This will provide an opportunity to assess the progress that has been made and whether the various components of the new data protection regime are fully operational after two years of application. To that end, the Commission will work with the European Parliament, the Council, member states, the European Data Protection Council, relevant stakeholders and citizens. 86 Article 97 Provisions. Regulation. gdpr regulation eur lex. gdpr uredba eur lex. gdpr testo eur lex. gdpr rendelet eur lex. gdpr 2016 eur lex. gdpr nařízení eur lex. gdpr article 28 eur lex. gdpr eur lex cz