ÖZGÜNLAW
PROTECTING YOUR INTERESTS

LAW BULLETIN

No. 4 September, 2020

We are glad to share September issue of our Law Bulletin which includes recent legal developments and news globally and in Turkey.

All the content herein is for information purposes only and please contact us for further information.

Editors:
Semra Gurcal
Burcu Celik

Implications from Schrems II Case: The Invalidation of the EU-US Privacy Shield Regime and Cross-Border Transfers of Personal Data

The recent decision on the Schrems II case [1], in the matter of compliance with the data protection principles of necessity and proportionality in the application of US law, became the most outstanding landmark case regarding international data transfer. The Court found that US surveillance law does not ensure the essential equivalent level of data protection provided within the EU. ***(Page 2)***

Everlasting Green Plants: Evergreening of Patents

When compared to other innovations, medical technologies and drugs undoubtedly have a more vital place in patent law. Even if the economic advantages of patents for inventors outweighs its other gained protections, when the patent subjects are medicines, drugs and other medical technologies, the perspective changes in a more sensitive way for public interest. ***(Page 7)***

A Doctor's Criminal Liability for Breaching A Patient's Right to Privacy

The contract between a doctor and her/his patient is formed when the patient consults the doctor for medical purposes and the doctor agrees to perform the medical intervention. Medical intervention may be defined as activities carried out by a doctor in order to diagnose, treat and if treatment is not possible, relieve, ease, slow or hinder the illness. ***(Page 12)***

Comparison of Patent and Utility Models in Turkish IP Law

- Which subjects are not deemed as invention and not allowed for protection by utility model in Turkey?
- What are the major differences between Patent and Utility Model?
- What are the 3 basic criteria sought for any invention to be patented? ***(Page 14)***

Q &A Session:
Brexit Transition Period and Intellectual Property Rights

- What is the effect of the Transition Period?
- Will the GDPR still apply when UK leaves the EU?
- Will any trademarks and designs, currently registered at the EU, be protected in the United Kingdom?
- How does Brexit affect international data transfers?
- How will the Existing Contracts be affected by Brexit? ***(Page 15)***

Recent News

Protectable Shape Mark:
Ritter Sport Chocolate ***(Page 11)***

Employer May Not Use Any Personal Data of Employees, Acquired Illegally, As A Valid Reason for Termination of Employment Contracts! ***(Page 11)***

A Pharmacy Owner Imposed with Administrative Fine due to Breach of Law on Protection of Personal Data! ***(Page 16)***

World Intellectual Property Organization (WIPO) launched "WIPO PROOF" to provide time stamping service for IP contents! ***(Page 16)***

IMPLICATIONS FROM SCHREMS II CASE: THE INVALIDATION OF THE EU-US PRIVACY SHIELD REGIME AND CROSS-BORDER TRANSFERS OF PERSONAL DATA

I. Introduction

The recent decision on the Schrems II case [1], in the matter of compliance with the data protection principles of necessity and proportionality in the application of US law, became the most outstanding landmark case regarding international data transfer.

The Court found that US surveillance law does not ensure the essential equivalent level of data protection provided within the EU; thus, the 'limited adequacy' decision which was adopted in 2016, so-called "EU-US Privacy Shield Framework" regarding EU-US cross-border data transfers, was invalidated at the CJEU.

According to the Court, US surveillance law was not proportionate and went beyond what was strictly necessary by granting access and feasibility to collect non-US citizens' personal data, and was inadequate by not offering any judicial redress against these activities.

With respect to the US law, the Court's decision, by invalidating the EU-US Privacy Shield, left any cross-border data flows on hold and in a legal void.

While the case before the CJEU involved only the US, where the decision deemed US protections insufficient, it means that data protection authorities (DPAs) will likely reach the same conclusion with respect to other trading countries such as Russia, China, India and Turkey.

As the European Data Protection Board (EDPB) stated, the threshold set by the Court for third countries also applies to all appropriate safeguards under Article 46 of the GDPR used to transfer data from EEA to any country. [2]

Aside from that, the ramifications of this decision do not only indicate to affect European citizens' access to products and services worldwide, and cause European companies to be hindered in competing across the global market, but also would affect health and pharmaceutical sectors, in cybercrime, fraud, and many other aspects of their lives since it directly interferes with the data flows.

On the other hand, EDPS considers this decision a constructive step to achieve actionable rights for everyone in the scope of data protection and states that it is more than a European fundamental right, but rather a fundamental right widely recognized around the globe. [3]

The EDPS also notes that it trusts the US will deploy all possible efforts and means to move towards comprehensive data protection and privacy legal framework, which genuinely meets the requirements for adequate safeguards.

As a direct result of the decision, relevant businesses and organizations in the US will have to reconsider how they would comply with the European data protection laws, as well as data exporters in EU.

Fortunately, there are several applicable GDPR mechanisms for cross-border data transfer, such as SCC decision in which the Court also emphasized, or binding corporate rules and derogations.

The Means of the Judgment

Under the General Data Protection Regulation ('GDPR') [4], cross-border data flows of personal data are limited.

According to Art.44, transferring personal data to a third country takes place only if the third country in question ensures an adequate level of data protection. Even though GDPR expresses the importance of data flows in regard to international trade and cooperation, the regulation also takes concern for the protection of personal data. [5] In accordance with that, data transfers to third countries and international organizations may only be carried out in full compliance with the European data protection law. Therefore, a transfer of personal data can only occur if the controller or the processor complies with the provisions of the GDPR.

With respect to the Schrems II decision, the CJEU considered reaffirming the importance of maintaining a high level of protection of personal data transferred from the EU to third countries. [6]

In that respect, the data transfer may only occur in the absence of an adequacy decision, where the personal data exporter in the EU has provided appropriate safeguards, on condition that data subjects have enforceable rights and effective legal remedies. [7]

The CJEU highlights twofold aspects as reasons for invalidation: US surveillance law provisions granting access to personal data related to European citizens that are not compatible with the EU data protection law, not requiring any independent approval from foreign individuals about whom the information will be collected.

The other being that not providing a reliable judicial remedy to non-US individuals whose data are collected by the intelligence authorities.

According to the Court, the lack of proportionality in US intelligence activities was concerning as they possess less clear legal standards in respect of "necessity in a democratic society to safeguard, inter alia, national security, defense, and public security."

II. Transfers of Personal Data to Third Countries or International Organizations

There are several ways of ensuring proper personal data security in regard to international data transfer according to the GDPR.

◊ Transfers on the basis of an adequacy decision; transferring the data to a third country approved by the European Commission ensures an adequate level of protection that is essentially equivalent to the European data protection laws.

◊ In the absence of an adequacy decision; applying proper data protection measures listed in Article 46 of the GDPR, which are signing standard contractual clauses adopted by the Commission, using binding corporate rules, and other measures.

◊ In case neither of these measures is applicable; the companies may transfer personal data in the absence of the appropriate safeguards outlined in Article 49 of the GDPR.

◊ Alternatively, making sure that the transferred data is depersonalized.

Standard Contractual Clauses

In addition to invalidating the EU-US Privacy Shield agreement, the Court also examined another widely used method for international data transfer, namely the standard contractual clauses, and considered the relevant legislation Commission Decision 2010/87 on Standard Contractual Clauses (SCCs) for the transfer of personal data to processors established in third countries valid.

SSCs are signed with the data recipients in a third country, and should only relate to data protection. [8] According to the CJEU, while SCCs are valid, the data controller is also required to assess the third country's legislation for sufficient protection, specifically regarding judicial redress, and the possibility of access to data from governmental institutions when signing such clauses in each case.

Thereby, the validity depends on whether if it includes effective mechanisms to ensure compliance with the level of protection equivalent to that guaranteed within the EU by the GDPR [9], which eventually means that companies will need to evaluate their use of SCCs.

According to the EDPB Statement of 17 July 2020, when conducting a prior assessment, the companies (the exporter) must consider the content of the SCCs, the specific circumstances of the transfer, and the legal regime applicable in the third country (the importer).

If the result of this assessment is that the third country does not provide the essential equivalent level of protection, the exporter may have to consider putting in place additional measures [10] to those included in the SCCs.

However, the EDPB is yet to come up with what these additional measures could consist of.

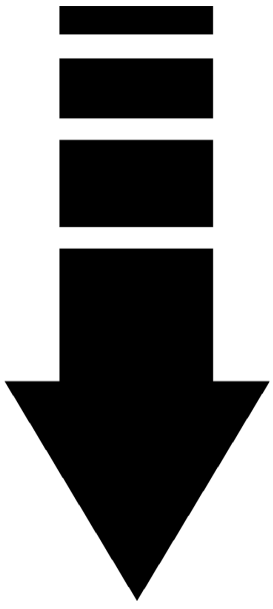
If the companies, as data exporters, intend to proceed with the data transfer outside the EEA, despite the negative assessment, then they are required to notify the competent authorities.

Another essential obligation we meet, along with this judgment, is the information obligation of both the importer and the exporter, in relation to change of legislation in the third country.

While the Court recalls the importance of complying with these contractual obligations, failing that, the exporter is bound by the SCCs to suspend or terminate the data transfer or to notify the competent supervisory authority if it intends to continue with the process.

According to Max Schrems [11]; the Court's decision aims to be a call to data protection authorities to become more proactive, and that SCCs can be valid if the Article 4 of the Commission Decision is applicable, where the competent authorities have the power to prohibit or suspend data flows to third countries, which only constitutes an adequate tool if the DPA has a duty to take action.

The EDPB also notes this provision in case the SCCs are not or cannot be complied within the third country, and the protection of the data transferred cannot be ensured by other means, in particular where the controller or a processor has not already itself suspended or terminated the transfer.



Binding Corporate Rules

The EDPB states that based on the fact that EU-US Privacy Shield was also designed to bring guarantees to data transferred with other tools such BCRs, therefore, US law will also have primacy over this tool, the Court's assessment applies as well in the context of BCRs.

This means that companies relying on BCRs must undergo a similar case-by-case assessment as the one used for SCCs.

However, since binding corporate rules do not constitute an extensible, broad-based solution compared to SCCs, it cannot be considered a definitive alternative.

Binding corporate rules constitute the only data transfer mechanism that carries individual regulatory approval, as supervisory authorities themselves participate directly in the review and approval of the BCRs.

By means that, the burden on assessing the adequacy of the safeguards rests with the supervisory authorities if a company uses BCRs, while the user of SCCs must make its own adequacy assessment according to the CJEU.

Therefore, it becomes unlikely that a supervisory authority would initiate an enforcement action against a data transfer that takes place on this basis.

According to the European Commission's guidelines [12], companies must submit binding corporate rules for approval to the competent DPA in the EU.

The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 of the GDPR. The competent authority communicates its draft decision to the EDPB, which will issue its opinion to be finalized. In accordance with the EDPB opinion, the competent authority will approve the BCRs.

In case of approval without any caveats, this will mean by implication, that the contractual safeguards are applicable for data transfer to all third countries in scope.

That said, approving BCRs with the caveat that individual data transfers are subject to case-by-case assessment would render the mechanism devoid of what makes them a convenient tool that provides legal certainty.

If the authority decides to reject, the applicant may apply to national courts for an appeal.

Derogations

It is also possible to cross-border data transfer on the basis of derogations set out in Article 49 of the GDPR.

The EDPB recalls, in the FAQ and later emphasized in the statement, that it issued guidelines on Art 49 GDPR derogations, and that such derogations must be applied on a case-by-case basis.

Derogations are only applicable in specific situations; therefore, they have a limited scope of applicability.

Moreover, derogations only apply where there are not any other transfer mechanisms available, and they serve as the last resort.

By that means, derogations only serve as an exception to the requirements for international data transfers.

In particular, they are only possible if these three key considerations are met; consent, necessity, and compelling legitimate interests.

According to EDPB, when transfers are based on the consent of the data subject, the consent should be taken explicitly, specific for the particular data transfer, and informed on the transfer's possible risks.

Aside from that, when the transfer is necessary for the performance of a contract between the data subject and the controller, it is only possible when the transfer is occasional.

Lastly, for the legitimate interest criteria, the transfer must be necessary for important public interest reasons.

The essential requirement for this derogation's applicability is that the reason must be "important public interest," which must be recognized in the EU or national legal framework, not the nature of the organization.

Even though the Court points at Article 49 to avoid creating a "legal vacuum" [13], derogations are not the ideal instrument for international data transfer, given their limited applicability and key criteria, and the necessity to be reviewed carefully

EVEN THOUGH GDPR EXPRESSES THE IMPORTANCE OF DATA FLOWS IN REGARD TO INTERNATIONAL TRADE AND CO-OPERATION, THE REGULATION ALSO TAKES CONCERN FOR THE PROTECTION OF PERSONAL DATA. [5] IN ACCORDANCE WITH THAT, DATA TRANSFERS TO THIRD COUNTRIES AND INTERNATIONAL ORGANIZATIONS MAY ONLY BE CARRIED OUT IN FULL COMPLIANCE WITH THE EUROPEAN DATA PROTECTION LAW. THEREFORE, A TRANSFER OF PERSONAL DATA CAN ONLY OCCUR IF THE CONTROLLER OR THE PROCESSOR COMPLIES WITH THE PROVISIONS OF THE GDPR.

before being relied upon as an alternative mechanism.

Therefore, it is unlikely that derogations would be in use to fill the gap that comes from the judgment.

Supplementary Measures

The Court highlighted that following an assessment, providing necessary supplementary measures is the primary joint responsibility of the data exporter and the data importer.

Moreover, the supplementary measures will be envisaged where they would have to be provided on a case-by-case basis as necessary, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.

By that means, the EDPB considers that companies to assess the supplementary measures to ensure that the law of the third country does not impinge on the adequate level of protection.

The EDPB also underlines that in a case where the assessment reveals that such protection is not guaranteed, it is required to stop or suspend the transfer.

However, the EDPB is still in the process of analyzing to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own.

Therefore, companies and organizations are required to find supplementary measures by themselves, pending future guidance from the EDPB.

III. Companies' and Organizations' Viewpoint

Companies are undeniably the most affected parties from these recent developments. Without EU-US Privacy Shield to facilitate them, how to maintain cross-border data transfer and relevant complications to these flows brings along a constrained process of evaluating their responsibilities.

To establish a lawful transfer, companies now have to conduct a thorough analysis in order to meet the accountability requirements.

The EDPB stated that it would not be providing a grace period for companies to continue to rely on Privacy Shield, indicating that the Court has invalidated the EU-US Privacy Shield decision without maintaining its effectiveness.

By means that, companies and organizations will have to be more aware and precautious of their responsibilities and obligations due to international data transfer during this transitional period.

The Court had already pointed to SCCs as the essential substituent data transfer mechanism and confirmed its validity.

According to the EDPB, whether or not the company can transfer personal data on the basis of SCCs will depend on the assessment.

This means that companies must assess the SCCs relevant to the data transfer taking into account the circumstances of the transfers and supplementary measures that could be put in place.

This assessment process would have to ensure that neither US law nor any other third country that data transfer would take place, impinges on the adequate level of protection.

As stated above, in case the company concluded that taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, then the company is required to suspend or end the transfer.

However, if the company intends to keep the data transfer to occur despite this conclusion, then there is an obligation to notify the competent supervisory authority.

Conducting Case-by-Case Analysis

With respect to the Schrems II case, the Court imposes on companies an obligation to assess if the level of protection in the recipient country is essentially equivalent to the level provided within the EU by GDPR.

As stated by the Court in its Press Release No.91/20[14],

> *"the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country."*

According to this provision, companies are now under the obligation of conducting an assessment when using other data transfer mechanisms since the Privacy Shield is no longer an option.

Evaluating each and every third country's laws for international data transfer is not only a challenging burden, but also practically troublesome for any organization from large corporations to smaller businesses.

How could it be expected that a company assesses the national security laws and the practices of their intelligence services accurately in order to send their HR data is another issue that needs to be solved arising from this situation.

To find a solution to that question, detailed guidelines must be published from the competent authorities.

In waiting for the guidelines and key aspects from the authorities on how the assessment should occur when transferring data to third countries, there are certain outlooks to handle the issue in a comprehensive manner.

In order to achieve that, the first step would be to carefully go around the SCCs and cooperate with the importer to ensure to address all the provisions partaking in the clauses.

Subsequently carrying out due diligence in following matters; the type of data subject to transfer, type of data subjects themselves, the purpose of data processing, the industry sector of the recipient, retention period, the law of the recipient country, and whether these laws bound the importer, and whether and to what extent the governmental agencies may require disclosure of data.

It is also practical and convenient to place additional measures of protection if necessary, to cure any deficiencies identified in the due diligence.

Aside from these procedures, data minimization or encryption is also subsidiary vice options to take into consideration.

The Activities of the Contractually Bound Processor

Current challenges after the Schrems II judgment also call for attention to controller-to-processor transfers of data.

Fortunately, the EDPB pays attention to processor activities in its FAQ, and further states that, the contract the controller has concluded with the processor in accordance with Article 28.3 of GDPR provides whether data transfers are authorized, or not.

In case of a matter relating to the processor's cross-border data transfer, authorization has also to be provided per purpose of processing and transfers.

Suppose the data may be transferred to the US, and neither supplementary measures can be provided nor derogations under Article 49 apply.

In that case, the only solution is indicated to be to negotiate an amendment or supplementary clause to the contract between parties to forbid transfers to the US.

The EDPB further elaborates that data should be stored but administered elsewhere than in the US.

If the data may be transferred to another third country, the controller should also verify the legislation of that third country to check if it is compliant with the requirements of the Court, and with the level of protection of personal data expected.

If no suitable ground for transfers to a third country can be found, personal data should not be transferred outside the EEA territory, and all processing activities should take place in the EEA.

Conclusion

While it is still an issue of concern how the consequences of this judgment will manifest in practice, companies that export and import data, will bear some residual risk for now.

The Court sets out quite a burden on businesses exporting data to other countries that wish to use SCCs; they must consider the law and practice of the country in which data will be transferred, especially if public authorities have access to the data. Additional safeguards, beyond the SCCs, may be required.

The EDPB also presses the competent authorities' part and duty to diligently enforce the applicable data protection legislation and, where appropriate, to suspend or prohibit transfers of data to a third country.

Companies can no longer treat contractual clauses as a mere formality; instead, they are now compelled to treat with care, and monitor their ability to comply with the contractual terms.

Apart from that, on a broader scope, concerning Schrems II decision, EU now possesses a quite narrow scope of movement in regard to international personal data transfer, and eventually, inflows international trade and communication.

Especially when it comes to relations with authoritarian countries such as Russia and China, it is not foreseeable to find a lawful basis for data flow to occur.

Considering the main remaining concerns of the absence of substantial checks and collection and access of personal data for national security purposes regarding US surveillance law [15], any other third country which may not be authoritarian in nature, but performs similar practices in surveillance enforcements such as Turkey, might also fall under the same scope of the evaluation.

In the meantime, the EDPB intends to continue playing a constructive part to provide assistance and guidance in building a new framework in the US that fully complies with the European data protection law, securing a transatlantic transfer of personal data that benefits EEA citizens and organizations.

For further information:
Att. Gokce Ergun
info@ozgunlaw.com

References:

1. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems https://noyb.eu/files/CJEU/judgment.pdf

2.https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

3. EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II") of 17 July 2020. https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2020-08_schrems_edps_statement_en.pdf

4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

5. GDPR Recital 100.

6. EDPB Statement of 17 July 2020.

7. GDPR Article 46.

8. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Recital 4.

9. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, adopted on 23 July 2020.

10. See, Supplementary Measures.

11. Schrems II: An In-Depth Interview with Max Schrems, Privacy Culture, 30 July 2020.

12. European Commission – Binding Corporate Rules (BCRs) & Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01)

13. Case C-311/18 – paragraph 202.

14. Court of Justice of the European Union, Press Release No 91/20, Luxembourg, 16 July 2020, Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems.

15. EU-US Privacy Shield – Second Annual Joint Review, adopted on 22 January 2019.

EVERLASTING GREEN PLANTS: EVERGREENING OF PATENTS

When compared to other innovations, medical technologies and drugs undoubtedly have a more vital place in patent law.

Even if the economic advantages of patents for inventors outweighs its other gained protections, when the patent subjects are medicines, drugs and other medical technologies, the perspective changes in a more sensitive way for public interest.

Public health and its progression are inherently a global goal, and both have high importance and priority on the international arena.

Since protection of human health, providing everyone access to health services and sufficient medical technologies in needed quantity and in required quality, providing these health services, medicines, medical equipment and devices in affordable costs and in a timely manner, are directly related to and a part of people's fundamental and inviolable right to life and to enjoy this right in the minimum required standard befitting with human dignity; even though there is no denying of the commercial interests and market competition in pharmaceutical and the medical device industry, providing equality in the access of medical drugs and devices is an essential aim to not to ignore.

However, development of medical technologies and drugs differs greatly from many other sectors with the risks they contain, requiring high-priced research and development activities, workforce, and time, the necessity of well-qualified workforce, fully-equipped R&D centres, laboratories and test environments, high priced materials, repeatedly made experiments and dealing with tons of long legal and procedural requirements not only during the stage of production and market release, but also as of the beginning of the research and development stage, as well as bearing all these material and moral efforts while keeping the probability of failure in mind because there is always a risk of all these high priced and full-fledged R&D to turn into a total waste if the products do not meet the legal requirements and/or targeted qualifications at the end of the day.

In this respect, despite all, some incentives and protections must be granted to these real and legal persons, who intend to make research, development and investment in medical technology sector, in order to promote technological progress in medical technologies, and to serve to the global aim of providing equal and affordable health services. Granting "patent rights" comes at first of these incentives.

Patent protection of an invention gives its holder a right to exclude others from exploiting the invention.

The rationale behind patent protection is to make the investment in R&D more attractive since patents can be used to prevent free enjoyers from launching copycat products, without even bearing the costs and efforts of R&D.

Patent is an exclusive right granted to the "inventor" in respect of an "invention" that is susceptible to industry, which may be a product or a process that provides a "new" and "inventive" way of doing something, or offers a new and inventive technical solution to a problem.

The owner of a patent may, in principle, exclude others in the territory covered by the patent from making, using, offering for sale, importing or selling the invention without her/his consent.

However, all these protections are provided for a limited period of time.

The term of patent protection is twenty years, and it is not possible to renew such period.

Even though patent protection promotes investments and R&D, it can also inhibit competition in drug market, for example, it can hinder market entry for generic medicines.

However, as mentioned above, the main and global goal behind patenting medicines is to provide everyone affordable health-care services.

That is why, distortion of competition in drug market is far beyond being only a competition problem, however, is crucial for providing access to affordable medicines and of course, for protection of the right to life.

Patent systems provide public access to technological information. The patent owner is obliged to disclose the claimed invention and all necessary information.

This system enables society to obtain information about the invention and formulations.

After expiration of the patent protection, generic companies can make use of the information and formulations, contained under patent documents, to produce their generic ones.

Generic medicines have a very important role in the production of affordable medicines since they tend to be way much cheaper than originator medicines, in other words, the medicines produced by the "patent owner" /or the licensee or the assignee who holds these patents related economic rights.

What is "evergreening"? Why is it defined as a problem?

It is very common for patent owners to carry out R&D activities to improve the effectiveness of their already patented medicines used for a specific cure.

There might be some changes found in the patented formulation which are known as incremental innovations.

These incremental innovations might be new dosage forms, improved and more durable storage characteristics, simplified route of usage, such as a change in the formulation derived the drug swallowed in pill rather than injection.

Incremental innovations are "further" steps taken on an already existing medicine which may make it more effective, simplified and/or durable, but in any case, a development which is not known in the body of existing knowledge, which is called as "prior art".

In principle, while the original patent will expire at the end of a specific time period and has to allow generic companies to compete duly across the market, patent holders can try to delay this by using different strategies such as investing heavily in the promotion of any new version of the medicines, and to convince doctors to switch patients to their patents' newer "incremental" versions so the doctors will not write out the generic medicines but the incremental versions in the prescriptions.

Another way employed by the originator companies in the jurisdictions where generics need an approved originator product on the market to refer to, they may withdraw the older patented version from the market which may affect market approval of older drugs' generic versions.

Sometimes the originator companies can also delay development or launch of such improved versions of drugs until the end of the patent term of the older main patented medicine to preserve their market position for a longer period.

It should be emphasized that, an incremental innovation on the patented medicine does not extend the term of the original patent.

However, the inventors can apply to patent the further innovation, and can grant the patents when the patentability criteria are completely met.

Granting a patent on an incremental innovation is independent from the patent of the original product. It has its own term of 20 years, and does not extend the term of the original patent.

While the second patent protects the modified form of the medicine, the patent protection of the original version will end upon the date of expiration.

In time, patenting the "incremental innovations" turned into a way for drug companies to maintain their dominancy across the market, and hold their patents of a specific drug for a very long period of time, by making dispensable changes on their innovations or very small improvements, displaying limited inventiveness with no added therapeutic value and granting 20-year-of patent protection.

This strategy used by drug companies to prolong their patented medicines are called as "**evergreening**".

The Commission on Intellectual Property Rights, Innovation and Public Health (CIPIH) defines evergreening as

"when, in the absence of any apparent additional therapeutic benefits, patent holders use various strategies to extend the length of their exclusivity beyond the 20-year patent term" (WHO, 2006(b)).

The European Commission has also identified another strategy used by pharmaceutical companies called "patent clusters" which is conducted by filing numerous additional patents for the same medicine.

Companies file a significant number of additional patents on variations of the same product, when the main patent is about to expire.

The Commission stated that this is a common way for the originator companies to keep generic companies out of the drug market and make it more difficult for them to evaluate whether it is possible to develop a generic version of the original drug without infringing one of the numerous patents filed around one medicine, in other words the "patent clusters".

The number of patents granted for the same drug raises the risk of potentially costly litigation for generic companies, which ends up with more expensive drugs, even if the ones produced by the generic companies.

How to differ "incremental innovations" from "evergreening" intentions?

It is crucial to avoid patents being used as barriers in market entry and competition. Demarcating the line between incremental innovations that confer real therapeutic advantages or manufacturing improvements, and those that offer no therapeutic benefits or remarkable improvements is not an easy task.

The governments should take consistent actions to avoid barriers to legitimate competition.

They can discuss to develop guidelines for patent examiners on how properly to implement patentability criteria and, if appropriate, consider changes to national patent legislation.

But how the line will be drawn between the modifications made for "evergreening" and the incremental innovations which really bring remarkable improvements? When does an adaptation of a first patented invention itself become separately eligible for a patent?

It is important to evaluate every individual invention claimed in a patent on its own merits.

Most innovations are already incremental by their nature as a result of technology which is naturally in progress in incremental steps.

To distinguish these natural progresses from valuable improvements, some additional criteria should be requested to be met, further than the inventive step/non-obviousness and all other patentability criteria already regulated under the applicable laws.

"Significant improvement in therapeutic efficiency of patented drugs" is an additional criterion discussed by the health-policy makers.

In order to prevent evergreening, the patent protection for incremental innovations should be granted only if they have sufficient additional therapeutic benefits.

If the therapeutic value of a product has been improved and significant advantages have been procured over what already exists in the prior art, these can be accepted as inventive steps for incremental innovations.

Besides additional criteria, the other patentability criteria of novelty, inventive step, and industrial applicability should also be ensured to be met.

It is strongly recommended for the countries to adapt a way to revise their patent legislations to prevent evergreening and help generic companies to be placed across the market.

Every country has the flexibility to design their national IP systems in accordance with their policy needs.

WTO Members are bound by the minimum standards set by the TRIPS Agreement, in cognizance of a country's economic, developmental, and other objectives.

This includes the right to define the patentability criteria. Countries may add additional criteria for granting incremental innovations or re-define the patentability criteria or spare patentability criteria for medicines and medical devices from other innovations.

If such solution would be adapted by countries, then the patentability criteria applied by examiners should also be checked to determine that whether they are in the line with the established definition and interpretation, or not.

Some regional patent offices have already set up search and examination guidelines to support the examiners' patentability check with a view to ensuring high quality of granted patents.

WIPO has published a collection of links to a range of patent offices' guidelines for easy access to this information, which is needed to be regularly updated.

However, it is still discussed whether the task of ascertaining incremental innovation meets the criteria for patentability offers therapeutic benefits or serves for "evergreening" and deters competition should be assigned to patent offices or would better be done by competition or health authorities.

Situation in Turkey

Even though the terminology "evergreening" has not been placed as a behaviour arising criminal and civil liability, it is quite possible for such companies to be liable under the terms of competition law.

Employers' Association of Pharmaceutical Industry declared a report on "The Barriers to Market Entry of Generic Drugs" whereby it was clearly stated that evergreening is obviously a problem for protection of patent rights, not only a problem seen in Europe or the drugs imported from Europe, but also in Turkey and between Turkish drug companies.

IT IS STRONGLY RECOMMENDED FOR THE COUNTRIES TO ADAPT A WAY TO REVISE THEIR PATENT LEGISLATIONS TO PREVENT EVERGREENING AND HELP GENERIC COMPANIES TO BE PLACED ACROSS THE MARKET. EVERY COUNTRY HAS THE FLEXIBILITY TO DESIGN THEIR NATIONAL IP SYSTEMS IN ACCORDANCE WITH THEIR POLICY NEEDS.

During the discussions before enaction of the Industrial Property Law numbered 6769, dated 22/12/2016 ("IPL"), there were many critiques on why special provisions on second medical use patents were not included in the bill of the new law. This view was supporting the idea of a restriction should be regulated to prevent granting patent rights for the modified medicines after the prior one's expiration.

However, the counter-view strictly supported that since there was no barrier for second medical use in Europe for European patents that have already been registered and Turkey was also accepting these patented medicines, secondary patenting and medical use should not be restricted under Turkish laws.

This view was also supporting that such restriction or barrier for second medical use would create a contrast between Turkish laws and European legislation, which should be definitely avoided to ensure our legislation's compliance with EU law, therefore the related regulation in EPC should be directly accepted.

However, the Supreme Court judges still concern regarding the tendency on prolonging the patent protection period by making very small modifications on drug patents, and support that instead of establishing a strict rule in patent law restricting the second patent use completely, the opportunity should be given to judges/practitioners to evaluate the aims and characteristics of such modifications and secondary patent in every different present case in their own terms.

However, in Article 138 of IPL, the invalidity conditions of patents are clearly stated. If the patent does not meet the requirements stated under Article 82, 83 and other procedural requirements stated in Article 138, the patent application shall be rejected. In any case, the evaluation of patentability shall be made according to Article 82 and 83; and any other claim shall not be taken into consideration in the evaluation of patentability.

In Article 82 (2) (c)), it is very clearly stated that "all treatment modalities including the diagnosis methods which are intended to be applied to human or animal bodies and surgical methods" as only the subject or the activity itself shall stay out of patentability. By this means, the judges may reject such patent claim if it only brings out a new treatment method, such as a new dosage regimen, for example.

Supreme Court supports the idea of evaluating such method patents from the "novelty" and "inventory step" point of view.

It should be strongly emphasized that invalidating all patents formed as new surgical and diagnosis methods shall constitute a clear breach of 82(6). Because IPL 82(6) clearly states that *"(6) The provision mentioned in subparagraph (c) of paragraph 3 shall not be applied to the products, especially the substances and compositions which are used in any methods that are mentioned in the same option."*

Because the purpose of this provision is ensuring the patentability of substances and preparations used in medical treatments to be evaluated apart from other diagnosis and treatment methods.

In other words, the existence of Article 82(6) precludes deeming invalid the secondary drug patent which contains a new component even if the secondary drug only differs from the previous one by bringing out a new treatment method.

That is why, since IPL and EPC provisions are clear, deeming the second drug patent invalid by the reason of that they only include a different dosage regimen or a different method of treatment is not a possible way to struggle with evergreening in Turkey.

However, the patentability evaluation can always be made in terms of other patentability criteria stated within the scope of IPL Article 82, 83 and 138. There is no doubt that evergreening is a global problem, and since every country also imports medicines and medical devices from other countries, evergreening cannot be struggled properly only by local law amendments.

Turkish patent law does not include any terms to prevent evergreening, even though Turkish IPL provides clear provisions on that treatment and surgical methods cannot be patented, it also provides that such term shall not be applied for the products, the substances and compositions which are used in any methods" which even closes our way to discuss the abovementioned idea about not granting patent rights for the secondary medicines which do not have any new non-therapeutic values. It would be a more decent decision to leave this part of evaluation to judges in order to let them decide in each case by obtaining expert reports indicating objective statements, instead of regulating a very clear rule to be applied as the same for all different medicines in different components.

Conclusion

The "evergreening" strategy is adapted by the originator companies to maintain their dominancy across the drug market as the patent holders, and to keep generic competitors out of the market for a longer term.

The main issue while preventing evergreening is to differ the adaptations that should be awarded and protected as a patent or be defined as anti-competitive behaviour.

Every invention should be evaluated on its own terms and checked if their patentability criteria are all met, which also includes the additional criteria to be determined by countries especially for the pharmaceutical sector.

Countries can revise their patent laws or their patentability guidelines and determine the definition and interpretation of patentability criteria for pharmaceutical patents, especially "therapeutic value" can be determined as a compulsory criterion for the improved products which claimed to be patented.

For further information:
Att. Burcu Seven
info@ozgunlaw.com

References:

WHO, WIPO, WTO, Health systems related determinants of Access, "Promoting Access to Medical Technologies and Innovation – Intersections Between Public Health, Intellectual Property And Trade", 2016.

WIPO, 2016, "Access to Medical Technologies and Innovation", The role of intellectual property in innovation and Access, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds114_e.htm

DRUG PATENT IN TURKEY, Aylin ACAR Selen YEĞENOĞLU, Ankara Ecz. Fak. Derg., 33 (4) 269 – 285s, 2004

İkinci Tıbbi Kullanım İstemlerinin Yeni Sınai Mülkiyet Kanunu Işığında Patentlenebilirliği

Aydın MUTLU, 26 Nisan Dünya Fikri Mülkiyet Günü Özel Sayısı

PROTECTABLE SHAPE MARK: RITTER SPORT CHOCOLATE

A precedent case on protected trademarks just landed on Germany's Federal Court of Justice (BGH). Chocolate manufacturer Ritter has the square shape of their Ritter Sport chocolate protected as a trademark. This trademark had been contested by Milka in court, arguing the square shape of the chocolate cannot be a characteristic feature, as it determines the nature of the goods themselves. Moreover, it had been argued that the shape of the chocolate is a functional feature since it makes it easier to hold and store.

Before the Supreme Court, it had been ruled that the shape of the chocolate bar is not an essential utility property for chocolates or a functional feature, but merely a design aspect, therefore protectable by trademark. Three-dimensional shapes, shape marks, or form marks may only be protected as trademarks if the shape does not constitute an essential characteristic of the product.

Accordingly, the appeal was also in Ritter Sport's favor. The Court stated that although the shape of the packaging may fully correspond to the shape of the goods or, in any case, come so close to it that it is justified not to distinguish between the shape of the packaging and the shape of the good.

Milka had opposed arguing that this constitutes a monopolization of shapes like the square for chocolate. However, the Court stated that the square shape of chocolate bars is not only one of the relevant basic shapes since most of the chocolate bars are manufactured in a rectangular shape.

According to the European Court of Justice, in the case of the shape of the product marks, goods and product packaging are equated only in the case of necessary forms of packaging, which do not have their own shapes such as liquid or powder. Even though this does not mean the packaging and the product is immediately protectable by trademark, it constitutes an applicable framework. In this particular case, Ritter Sport was known for the square shape of its packaging and product. By that means, the Court also recognized Ritter Sport's marketing strategy and advertising slogan for the product, "Square. Practical. Good."

The shape of a product could only be excluded from trademark protection if it provides the product a significant value, which may indicate an issue in terms of competition. However, in this particular case, it had been stated that the square shape of the packaging does not possess any artistic value or does not add a significant one; therefore, the Court ruled the square shape is protectable by trademark.

References:

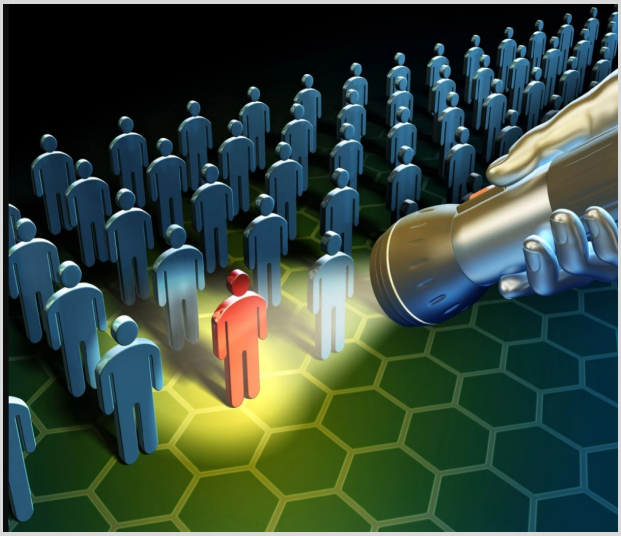
1. Judgement of Ritter Sport, 14.05.2020
2. Pressemitteilung des BGH vom 23. Juli 2020, I ZB 42/19 und I ZB 43/19
3. Judgemtent of BPatG, december 2018, 25 W (pat) 79/14

EMPLOYER MAY NOT USE ANY PERSONAL DATA OF EMPLOYEES, ACQUIRED ILLEGALLY, AS A VALID REASON FOR TERMINATION OF EMPLOYMENT CONTRACTS!

The Court of Cessation, the Turkish supreme court of appeals, issued an order on 07.05.2019 whereby it was stated that employers may monitor the computer activities of any employee to the extent that preliminary information is provided to the same by the employer. It was further stated that otherwise, the personal data of the employee would have been acquired illegally, and that the employment contract of the same may not be terminated with a valid reason based on the justification of such personal data.

The related part of the said order reads as follows:

> *"Employers may, at all times, monitor and follow-up its own employees on electronic medium as a direct result of its right to manage the same. However, the requirement of provision of preliminary information thereof to the employee shall be sought. Any failure to provide information to the employee about such monitoring or follow-up action, or monitoring thereof in secret shall be deemed illegal even if any data, acquired in consequence of such actions, clearly shows that the employment contract has been violated by the employee. Accordingly; in this present case, it should be awarded that any information, acquired by the employer in consequence of any secret monitoring actions, may not be claimed as a valid reason for termination."*



(The order, bearing the Basis Number 2017/21857, the Decision Number 2019/9884 and dated 07.05.2019, of the 22nd Civil Chamber of the Court of Cessation)

A DOCTOR'S CRIMINAL LIABILITY FOR BREACHING A PATIENT'S RIGHT TO PRIVACY

I- Introduction

The contract between a doctor and her/his patient is formed when the patient consults the doctor for medical purposes and the doctor agrees to perform the medical intervention [1].

Medical intervention may be defined as activities carried out by a doctor, in accordance with medical science, in order to diagnose, treat and if treatment is not possible, relieve, ease, slow or hinder the illness.

Once the contract is formed, the doctor is under the obligation to act carefully, examine, diagnose, treat the patient, and protect the patient's privacy.

A doctor has to examine the patient and collect her/his medical history before applying the relevant treatment. If the findings are inadequate for a decent diagnosis, the doctor will ask to run medical tests that require various samples to be taken from the patient.

Shortly, any data concerning the patient's medical status either retrieved directly by the patient or through tests, constitutes a person's "health data" which is a special category of "personal data".

The Law on Protection of Personal Data nr. 6696 defines personal data as "all the information relating to an identified or identifiable natural person";

The term "Health data" is defined as

> *"Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.*
>
> *This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (9) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."*

under the regulation (EU) 2016/679 of the European Parliament, and of the Council.

II- Legal Basis of A Patient's Right to Privacy

Article 6 of the European Charter of Patients' Rights sets out:

> *"Every individual has the right to the confidentiality of personal information, including information regarding his or her state of health and potential diagnostic or therapeutic procedures, as well as the protection of his or her privacy during the performance of diagnostic exams, specialist visits, and medical/surgical treatments in general."*

Adopted by the 34th World Medical Assembly, Declaration of Lisbon on the Rights of the Patient proclaims that

> *all identifiable information about a patient's health status is confidential even after the patient's death, and that*
>
> *it may be disclosed upon explicit consent, only.*

Article 6 of the Patient Rights Regulation adapts that a patient's private and family life may not be intervened unless there is either a legal or medical necessity therefor.

Section 6 of the Law on Protection of Personal Data nr. 6698 deems all health-related data a special category of personal data, and sets out that it may not be processed without explicit consent, except for any purpose of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of non-disclosure, or any authorized institutions and organizations.

As it is seen, all health-related data are considered extremely confidential, and subjected to strict protection policies both nationally and internationally.

III – Sources of Criminal Liability of A Doctor Disclosing A Patient's Personal Data

The section 136, titled "Illegally obtaining or delivering of data", of the Turkish Criminal Code nr. 5237 reads as follows: *"Any person who illegally delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years."*

The section 258, titled "Disclosure of office secrets", of the Turkish Criminal Code nr. 5237 reads as follows: *"Any public officer who discloses or publicize the confidential documents, decisions and orders and other notifications delivered to him by virtue of office, or facilitates access to such information and documents by third parties, is punished with imprisonment from one year to four year."*

These two sections are considered to be possible sources of a doctor's liability for breaching her/his patients' privacy.

It should be stated firstly that this distinction applies to doctors who perform public duty and are therefore public officers as "disclosure of office secrets" may only be committed by public officers.

According to the Court of Cassation, doctors who work at private hospitals and/or private clinics are not considered to be public officers [2].

IV- Criminal Liability of A Doctor Disclosing A Patient's Personal Data

The old version of the Turkish Criminal Code nr. 765 involved the offence "disclosure of a professional secret" which is very similar to "disclosure of office secrets", set out under the current version of the Turkish Criminal Code nr. 5237. According to Cambridge Dictionary, a secret is "*a piece of information that is only known by one person or a few people and should not be told to others*" [3]. For a secret to be deemed professional or office-related, it has to be delivered to the public officer upon trust in her/his title or professional reliability.

As it is defined under the introduction part hereinabove, personal data means as follows: *"Any data relating to a natural person is regarded as personal data."* Compared to the term "secret", "personal data" clearly contains a broader definition [4].

Trying to catch the worldwide legal trend regarding data protection, the current version of the Turkish Criminal Code nr. 5237 has deemed "illegally obtaining or delivering of personal data" a criminal offence for the first time. However, "disclosure of office secrets", with minor changes made, was adapted from the old version of the said regulation.

A personal data does not have to be a secret. However, a piece of information known to everyone cannot be categorized as personal data.

Since a doctor is legally obliged to look out for her/his patient's interests at all times, it would be the best to adopt the criteria "information that has to remain a secret due to the patient's interests" [5].

It might be argued that "disclosure of office secrets" will be applicable for doctors who work at public hospitals as it pertains solely to public officers and hence more specific compared to "illegally obtaining or delivering of personal data".

On the other hand, considering that the legislator made a new rule covering almost the same subject and broadened the aspects of the object and the legally protected value of the crime, it would be right to assume that they wanted to provide a further scope of protection.

It is also important to note that the section 137 of the current version of the Turkish Criminal Code nr. 5237 states that if the person who illegally delivers data to another person; a) "is a public official misusing her/his power derived from her/his public post" or b) "by benefiting from the privileges derived from a profession or trade", these are the aggravated forms of the main crime.

This also indicates that the legislator intends to apply the said section to public officers. In addition, a patient does not share her/his medical data with the doctor because of the trust generated by the doctor being a public officer.

What the patient trusts is that the doctor will use the information provided to her/him only for medical purposes, and will not breach her/his privacy by delivering it to a third party unless legally or medically so required.

This fair belief is due to the nature of the relationship between a patient and her/his doctor. In this sense, it is unfair and against the "equality principle" to make a distinction between doctors who are public officers and who work privately [6].

In consequence, a doctor who illegally disseminates or delivers her/his patient's personal data to a third party, either working privately or in a public hospital, will be punished pursuant to the section 136 of Turkish Criminal Code. The penalty will be increased pursuant to the section 137 due to the fact that the doctor acquired the illegally delivered information from her/his profession.

For further information:
Att. Ezgi Ozdemir
info@ozgunlaw.com

References:

1. Hakan Hakeri, "Tıp Hukuku", 4th Edition, Ankara, 2012, p. 43

2. The Decision, dated 30.05.2018, numbered 2018/6166 and bearing the File Number 2016/9578, of the 12th Penal Chamber of the Court of Cassation

3.https://dictionary.cambridge.org/dictionary/english/secret

4. Sabire Senem Yılmaz, "Tıp Hukukunda Kişisel Verilerin Açıklanması Suçu", Ankara, 2014, p. 85

5. Handan Yokuş Sevük, "Tıp Ceza Hukukunda Kişisel Verilerin Açıklanması", Tıp Ceza Hukukunun Güncel Sorunları, Türkiye Barolar Birliği Yayını, Ankara, 2008, p. 796

6. Hakeri, ibid, 750

COMPARISON OF PATENT AND UTILITY MODELS IN TURKISH IP LAW

1- Which subjects are not deemed as invention and not allowed for protection by utility model in Turkey?

* Discoveries, scientific theories and mathematical methods.
* Plans, rules and methods for mind activities, business activities or games.
* Computer programs.
* Products with aesthetic qualities, literary and artistic works and scientific works.
* Presentation of information.

2. What is a patent?

Patent is entitlement of an inventor to the right to manufacture, use, sell, have it manufactured under its own license (to license) and import the respective product/method which brings a solution to any specific problem of the inventor.

The official certificate, which proves that such rights are held by the inventor, is called as the "Patent Registration Certificate".

The inventor may put its own product/method, which exceeds the state of the art in respect of the inventive step, under protection through patent registration.

3- There are 3 basic criteria sought for any invention to be patented, namely:

ι) NOVELTY
ιι) INVENTIVE STEP
ιιι) INDUSTRIAL APPLICABILITY

Novelty:
Any invention which is not included in the state of the art is considered novel. In other words, the respective invention must have not been expressed or used in writing, verbally or in any other fashion in a manner to be accessible publicly all around the world.

Inventive Step:
Invention is defined as a solution to any and all kinds of specific problems, which can be produced and/or used in any branch of the industry, including agriculture. In short, anything which has been created for the first time is called as invention. An invention shall be considered as involving an inventive step if, having regard to the state of the art, it is not obvious to a person skilled in the art.

Industrial Applicability:
Industrial applicability means that any invention bears the feature of being practical rather than being corporate, in its entirety.

4. Differences between Patent and Utility Model

While patents are required to have the above-mentioned 3 criteria, the second criterion of "INVENTIVE STEP" is not sought for Utility Models, which means that it is sufficient for any product, covered by the Utility Model, to be NOVEL, without any requirement to involve the INVENTIVE STEP. In this regard, Utility Model is also called as "petty patent".

5. Differences with respect to protection system and protection periods:

In respect of Patents:
Since the patent certificate is granted based on an examination report proving that whether the application has the patentability criteria (novelty, inventive step, industrial applicability), or not, it ensures a more well-established and longer protection. Patent certificates provides a protection period of 20 years, which is not possible to be extended any further.

In respect of Utility Models:
There is not any examination process, unlike patents. Therefore, it takes a shorter period of time and costs lower to obtain a certificate for utility models, compared to patents. Under this system, protection is provided based on the examination report.

Utility Model certificate provides a protection period of up to 10 years, which is not possible to be extended any further.

Briefly;
The major differences between Patent and Utility Model are as follows, as explained hereinabove: While the protection period of patents lasts for 20 years, the protection period of utility models lasts for 10 years, and it is not required to conduct researches and examinations to obtain the Utility Model certificate (except a brief search on the availability of the drawing), unlike the Patent certificate.

Researches and examinations are conducted to determine that whether the respective products have been manufactured before, or not while the Patent certificate is obtained. Therefore, it is much easier and more affordable to obtain the Utility Model certificate than to obtain the Patent certificate.

For further information:

Serdar Darama, Trainee Lawyer
Burcu Celik, Translator
info@ozgunlaw.com

Differences between Patent and Utility Model*

	Patents	Utility Models
Novelty	+	+
Inventive Step	+	-
Industrial Applicability	+	+
Methods and Products Created through methods	+	-
Pharmaceutical Products	+	-
Biotechnological Inventions	+	-
Chemical and Biological Substances	+	-
Research Report	+	+
Examination Report	+	-
Protection Report	20 years	10 years

* Turkish Patent Institute (https://www.turkpatent.gov.tr/TURKPATENT/?lang=en)

Q&A SESSION: BREXIT EFFECT

The UK formally left the EU on 31 January 2020, as known. The transition period, scheduled between 1 February 2020 and 31 December 2020 in order for completion of changes to take place in many legal and political issues, will end in around 4 months.

United Kingdom Intellectual Property Office (UKIPO) released elaborate statements on this process.

Above all, the EU law is kept being enforced same as before during the transition period. Therefore, the EU trademarks and design will remain to be effective across the UK during the transition period.

⇨ Will any trademarks and designs, currently registered at the EU, be protected in the United Kingdom?

Trademarks and designs, which are currently registered, and which will be entitled to be registered until the end of the transition period, will be converted into national trademarks and designs by the UKIPO during this period, which means that the current registered owners of any EU trademark and design do not need to file a separate application for registration in the UK.

⇨ Will the actions, taken at the EU, be applicable for the nationally protected trademarks and designs at the UK?

NO. All converted trademarks and designs will be deemed registered at the UK as of 21 January 2021.

Therefore, any and all actions (such as renewal, transfer, etc.) will be performed and carried out at the UK in compliance with the UK law independently of the EU thereafter.

☛ *So, we highly recommend you to not to forget performing the renewal actions at the United Kingdom!!!*

Trademarks and designs need to be renewed at the UKIPO so that they will remain applicable at the United Kingdom.

⇨ What should the owners of trademarks and designs, for which an application has been filed at the EU, but which have not been entitled to registration yet at the end of the transition period, do?

A 9-month period has been prescribed with respect to the applications for such trademarks and designs in a manner to start as of the end of the transition period. The applications for trademarks and designs at the EU will be had registered as national applications with the date of application at the EU maintained, to the extent that the application fee is paid at the United Kingdom.

☛ *UKIPO will add the code UK009 before the trademarks and designs of EU origin to facilitate follow-up of trademark and design registrations, and to prevent any possible confusion.*

⇨ What will the status of patents, currently registered at and before the European Patent Office (EPO), be?

European Patent Office (EPO) is an international organization established based on the European Patent Convention. It is independent of the EU and has 38 member countries with 27 of them being the EU member countries, and the remaining 11 countries (including the United Kingdom) not being the EU member countries.

Therefore, the Brexit process will not have any effect on the patents registered at and before the European Patent Office. Your such patents will be kept being protected at and before the EPO member countries including the United Kingdom.

⇨ What is the effect of the Transition Period?

During the transition period which will continue until the end of 2020 the GDPR will continue to apply in the UK.

⇨ Will the GDPR still apply when UK leaves the EU?

The GDPR is an EU Regulation and it will no longer apply to the UK from the end of the transition period. For the companies operating inside UK, UK data protection law ("DPA") will be applied.

However, GDPR will still apply to any organizations in Europe who send you data, how to transfer personal data to the UK in line with the GDPR.

⇨ What will the UK data protection law be?

The Data Protection Act 2018 (DPA 2018) will continue to apply.

⇨ How does Brexit affect international data transfers?

Since UK is no longer an EU member state, the UK has been reclassified as a 'third country'. From the end of the transition period, unless the EU Commission makes an adequacy decision, GDPR transfer rules will apply to any data coming from the EEA into the UK.

⇨ How will the Existing Contracts be affected by Brexit?

Brexit has no direct effect on the contractual relations. However, at the end of the transition period, transfers of data from the EU to the UK will be subject to local transfer requirements in the sender's country.

Therefore, in international relations, UK companies might be asked to comply with additional safeguards for the international data transfers. Then, it becomes important to review the continuing contracts since some clauses may require revisions after Transition period.

A PHARMACY OWNER IMPOSED WITH ADMINISTRATIVE FINE DUE TO BREACH OF LAW ON PROTECTION OF PERSONAL DATA!

The incident, constituting the subject matter of the decision, is as follows: A petitioner applies with the Provincial Directorate of Health, claiming that a pharmacist is uncapable of practicing due to health issues and therefore lacks the knowledge and skills required by the job, and should not be allowed to run and be in charge of a pharmacy for the benefit of public health. Attached to the petition, there are "Medula Pharmacy" documents that disclose some diagnostic and pharmaceutical information belonging to the afore-mentioned pharmacist.

"Medula" is an electronic information system run by the Social Security Institution to collect healthcare data and perform billing based on such data.

"Medula Pharmacy" is a system that monitors if the drug prescriptions, received by General Health Insurance right holders from pharmacies contracted with the Social Security Institution, are in accordance with the rules, as set by the Social Security Institution, or not.

Pharmacies contracted with the Social Security Institution are authorized to make use of this system and can log into the system with their ID numbers and access all personal data, and sensitive personal data. Therefore, pharmacists can process data through the Medula System.

Provincial Directorate of Health reports the incident to the Personal Data Protection Board as the petitioner's spouse is also a pharmacist, and it is highly likely that the Medula Pharmacy documents, attached to the petition, have been obtained from the spouse's pharmacy.

Personal Data Protection Board adopted a decision, stating that the pharmacy failed to take necessary actions to prevent third parties from accessing to Medula System under the scope of the contract between the pharmacy and the Social Security Institution.

The pharmacy, breaching the Section 12 of the Law on Protection of Personal Data, received an administrative fine of TRY 60,000.00 pursuant to the Section 18/1 thereunder.

The Board also denounced to the Public Prosecutor's Office that the petitioner, who used Medula Pharmacy documents belonging to the respective person, acquired the respective personal data through illegal means, resulting in the breach of the Section 136 of the Turkish Penal Code.

(Decision, dated 07.05.2020 and numbered 2020/355, of the Personal Data Protection Board)

WIPO PROOF: DIGITAL EVIDENCE FOR INTELLECTUAL PROPERTIES

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

World Intellectual Property Organization (WIPO) launched "WIPO PROOF", a new online application, on May 27, 2020, starting to provide time stamping service for contents which might be subject to intellectual property.

This service will enable to record existence of any intellectual property contents at WIPO along with a certain date and time, and it may be used as evidence in any legal disputes.

This brand-new service is, undoubtedly, a groundbreaking development for protection of intellectual property rights not registered at any competent authority yet.

Anyone can access WIPO PROOF's secure online website to request a WIPO PROOF token for a specific digital file.

WIPO does not read the file's contents or store a copy of it. WIPO PROOF's secure, one-way algorithm interacts locally with the requestor's browser to create a unique digital fingerprint of the file.

WIPO PROOF provides reliable and verifiable evidence in case of disputes and litigation over the existence and integrity of the digital file and its related IP rights.

For further information: https://wipoproof.wipo.int/wdts/

Sülün Sok. No:8 34330 1.Levent Beşiktaş / TURKEY
Phone : +90 212 356 3210 (pbx) / +90 212 325 2307 (pbx)
Fax : +90 212 356 3213
E-mail : info@ozgunlaw.com
Webpage: www.ozgunlaw.com

Follow us!