03

E-newsletter

September
2013

Directorate for Personal Data Protection

In this issue:

Dear readers,

Hereby we present you the third edition of the e-newsletter of the Directorate for Personal Data Protection of the Republic of Macedonia.

The mission of the Directorate for Personal Data Protection is to provide an effective system for each individual in the exercise of the right to protection of personal data by monitoring the legality of the processing of personal data.

To that end we put great effort to continuously improve the situation, to express firm determination to achieve even better results, to show that we are deeply motivated and open to cooperation, following the interest of democracy in a civilized society.

The issue of protection of personal data and the issue of protection of privacy are part of the common area of human rights which are always a challenge for institutions dealing with these issues.

We do hope that in this way we will expand your knowledge in the field of protection of personal data, so that we will all contribute to strengthening of cultural awareness and respect for the right to privacy.

In each new edition you will have an opportunity to learn more about the activities of the Directorate, conducted trainings, conducted inspections and will inform you on how to act in case of misuse of your personal data.

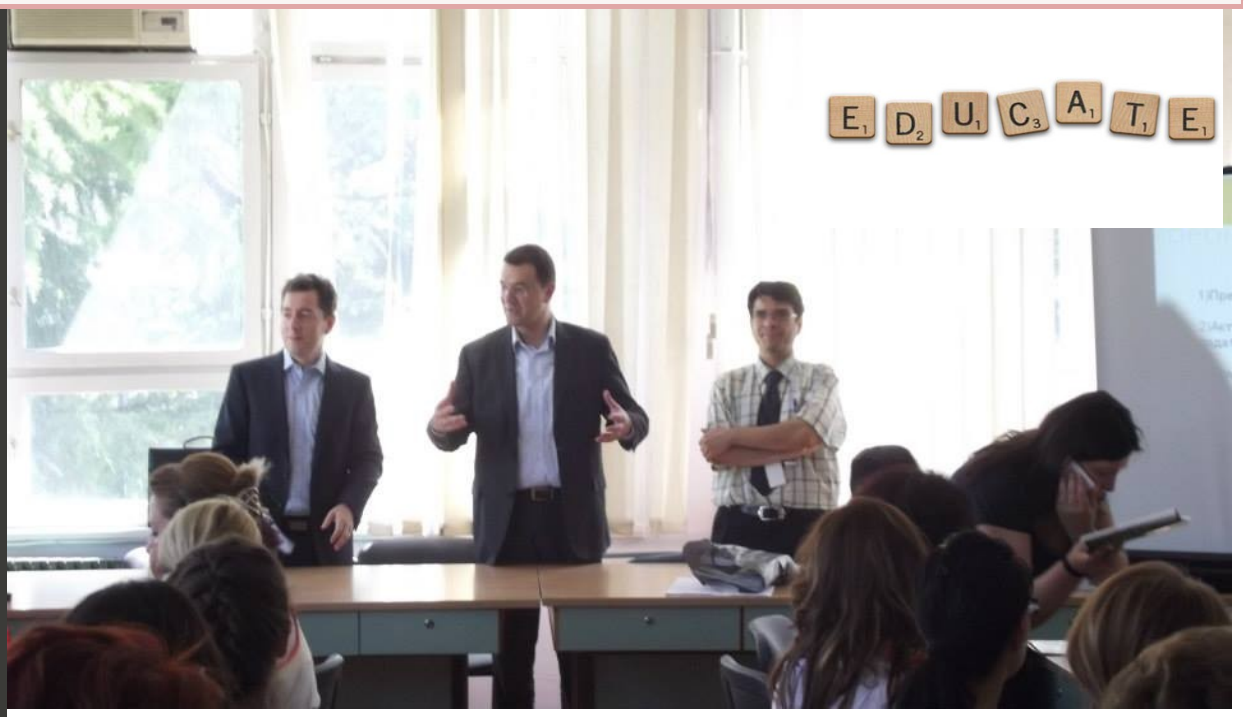
Director,

Dimitar Gjeorgjievski

"I own my privacy"

DPDP

ДЗЛП



Borivoj Kos,

Team Leader of the Project

Respect for human rights is a fundamental criterion that reflects the role of the citizen in society. Citizens need to know their rights and freedoms in order to protect them in case of violation. Enriching the educational system with the right to privacy and protection of personal information is extremely important to create the right culture among students, teachers and parents.

The actions taken so far have encouraged and fully supported the teachers to share their experiences and views on raising awareness about the right to privacy and protection of personal data in these groups and to create specific curricula and content. The new curricula will help students to recognize the dangers of unauthorized disclosure or misuse of their personal information, especially to learn how to use social networks safely and be careful with whom they make friends and share private photos.

IPA 2009 Project in sector— Education

Within IPA 2009, on June 25 this year at High School "Vasil Antevski Dren", Skopje, a promotional event was held for the initiation of the Project: "Sustainable system for continuous primary and secondary education in the principles of protection of personal data", whose beneficiary is the Directorate for Protection of Personal Data.

The project is aimed at primary and secondary schools and has it goal to raise awareness and educate the teachers about the protection of personal data. During the implementation of this project specific materials and documents shall be prepared for the right to protection of personal data in educational purposes in primary and secondary education, which will contribute to raise the knowledge of practical implementation of the legal provisions of personal data protection, trainings will be also organized for teachers, targeting the educational system in the country in the field of protection of personal data. The project activities will enable the identification of the knowledge of the educators for the right to privacy and their education on this issue.

During the ongoing activities of the project, several teaching lectures from primary and secondary education will be selected into which the curricula shall be implemented on the right to protect personal data and the same will be delivered in 10 previously selected pilot -schools.

Given the importance of the educational personnel, especially the fact that the teachers are the target group that can directly affect the behavior of young people in social networks, the exchange of personal data in/ out of school, the Directorate pays special attention to the interest of this group. Thusly, the Directorate, through a sector-oriented approach to education promotes the education sector as an important issue of great social concern.

At this promotional event representatives of the EU Delegation in Macedonia, d. Elvis Ali, the Director of the Directorate for Personal Data Protection, Mr. Dimitar Gjeorgjievski, had their address, as well as part of the Project Team.

PROMOTIONAL !

PROTECT YOUR PRIVACY AND THE PRIVACY OF YOUR CLIENTS AND FAMILIES

CERTIFIED TRAINING FOR DIGITAL SECURITY OF COMPUTER USERS

The development of modern technology poses questions on a daily bases about the security of Internet communications and data protection in general. The Directorate for Personal Data Protection of the Republic of Macedonia considers that it is of particular interest to increase citizens' awareness on these issues and finding way to its implementation. The signing of the Memorandum of Understanding between the Directorate for Personal Data Protection (www.privacy.mk) and EC Council (International Council of Electronic Commerce Consultants; www.eccouncil.org) provided an opportunity for the two entities to expand the scope of cooperation by organizing training and education for controllers and processors of personal data as well as for all computer users who are in daily contact with sensitive information, in accordance with the Annual program of the Directorate. The Government of the RM, through the Directorate for Personal Data Protection is one of the first in the world to sign a Memorandum of Cooperation with the EC-Council. For that purpose on 31.07.2013 was signed the Memorandum with "SEMOS Education", which is the only authorized training center of EC-Council (International Council of Electronic Commerce Consultants) in the Republic of Macedonia.

DATA PROTECTION OFFICERS!

- **Who is responsible for IT security in your company or institution?**
- **Can financial and personal information of your customers be abused because of insufficient knowledge of your employees?**
- **Are your employees able to identify IT security threats?**
- **Are they authorized to take proactive steps against these threats?**
- **Did you know that Apple and Deloitte recently were victims of hacker attacks?**
- **Do you think you will be able to avoid or "escape" from such threats?**

Delivery of Training:

from 01– 04 October 2013,

In the premises of the Directorate for Personal Data Protection

Introductory:

1. Applying the principles of data protection
2. Technical and organizational measures to ensure the confidentiality and protection of personal data

Curricula of Trainings:

Module 01: Security Bases

Module 02: Securing Operating Systems

Module 03: Protection of systems using antivirus

Module 04: Data Encryption

Module 05: Backup of Data Disaster Recovery

Module 06: Internet Safety

Module 07: Securing network connections

Module 08: Securing Online Transactions

Module 09: Securing Email Communication

Module 10: Social engineering and identity theft

Module 11: Safety on social networks

Module 12: Safety Information

Module 13: Securing mobile devices

Register HERE

- Duration: 16 hours - 4 days
- Promotional price: 7.500,00 in denars.
- Certificate: After training you can be tested for CSCU (112-12) acquiring the title "Secure Computer User Specialist" (CSCU).
- Provision of Six months access to EC-Council Lab.
- Delivery of training is in the premises of DPDP, blvd. Goce Delcev 18, floor 14.
- Execution of Payment in SEMOS Edukacija or account no: 300000000470777

Initiative for an irregularity inspection you can find it HERE

SMILE AS YOU DRIVE!

Author: Elena Stojanovska, M.A.

The trend of placing cameras at intersections and other selected places at the crossroads continues, and the goal expected to be reached is having safer traffic. At the same time, the question is whether this way of monitoring the behavior of traffic participants is allowed and under which legal norms is implemented.

The provisions of the Law on Personal Data Protection ("Official Gazette of RM" no. 103/08, 124/10, 135/11) apply to the processing of personal data by video surveillance, unless by other law not provided. The controller, in this case the Ministry of Internal Affairs of the Republic of Macedonia may conduct surveillance if it is necessary to protect the life or health of people, protection of property, protection of life and health of employees due to the nature of the work or providing control over entry and exit of official or business premises.

Pursuant to the “Law on safety of traffic on roads”, article 411 ("Official Gazette of RM" 123/2012) the Police is authorized to set up recording devices in public places on traffic roads and where consideration that offences from the field on offense road traffic may occurred/happened, in accordance with the Law.

“Recording” in terms of this Law implies constant video surveillance on public places. Recording can be done with special vehicles of the Ministry of Interior equipped with special devices for this purpose. The recorded material is kept in the Police for six months, after which the material is destroyed, except material considered as evidence in criminal or misdemeanor proceedings, which are handled in accordance with the Law.

Despite the existence of this legal basis, the controller performing video surveillance is required to highlight the information that will have to be clearly visible and prominent in a way that allows data subjects to know about the performance of video surveillance.

The Ministry of Interior of the Republic informs that: "Monitoring Center is one of the most modern one, made by an EU model used in the metropolis. The Center meets all international standards in terms of access and in terms of processing and storage of data.

The Center has exclusively trained and professional staff whose priority in their work is respecting human rights and strict adherence to fully respect the laws of the Republic of Macedonia. There are currently no comments on the operation of the project "Safe City" and the staff there.

Even when installing security video surveillance, the Ministry of Interior designated the locations where the cameras are placed, but unfortunately negligent citizens removed most of them. But despite of that the MOI continues regularly to inform citizens about the video surveillance through the media, and also using its website."

Did you pass the test?!

Implementation of the Law on protection of personal data, as well as by-laws relating to inspection, provided substantial institutional strengthening of the inspection function of the Directorate, as well as strengthening the preventive function by having the controller to complete the **Checklists (Check List)** before commencement of supervision on the spot.

At the same time, it does provide proactive participation and self-estimation opportunity for the controllers or processors in the process of ensuring consistent application of regulations for personal data protection.

The Inspections are planned by sector based approach, through annual programs delivered, and in the reference period is currently being implemented through monthly implementation plans. In the reporting period the priority areas in which inspections were conducted are: accounting services, telecommunications, healthcare, trade, justice and administration (PPO, notaries, Lawyers, etc.).

In the last quarter of the year, we have acted upon 89 cases, out of which 62 inspections are conducted under the adopted Program and Plan for supervision and 27 cases by performing an ad-hoc/irregular inspection.

According to the Law on Personal Data Protection ("Official Gazette of the RM" no. 103/08, 124/10, 135/11), an ad-hoc inspection is on the basis of initiative submitted by the state authorities, natural or legal person, as in the case of suspicion of the inspector for violation of the provisions of this law.

Ad-hoc inspections are performed in the case after an initiative submitted pursuant to Article 18 of the Law on Personal Data Protection.

The fact that in one third of the cases, i.e. in 27 cases it is acted upon notification of a violation of the right to protection of personal data by individuals, represents an interesting fact-finding; mostly it is in the field of internet, video surveillance, electronic communications, broadcasting, trade, banking and heat supply.

For the same period (from May to July 2013) it is characteristic that the number of applications sent by citizens is increased, especially for injuries resulting from violations of guaranteed right to protection of personal data, which confirms the fact that awareness of the protection of personal data is raising among citizens.

Both at controllers, i.e. processors the level of awareness is increasing about the need to know about the latest data protection legislation changes and their implementation as an obligation and necessity in institutional terms.

Thusly, protection of privacy and personal data are no longer interpreted only as a basic human right, but also as an important need in everyday modern life.

TRAINING in the DPDP

The protection of personal data is an area that is constantly progressing, builds and monitors development trends of technology.

Continuing education for the implementation of the personal data protection principles is one of the ways to familiarize controllers with legislation in this area.

Trainings on secrecy and protection of the processing of personal data are carried out by predetermined modules: one general and 16 specialized modules depending on the area controllers and processors are work related.

Information on Training Program for provision of secrecy and protection of the processing of personal data and **Request** for applications for training can be found at the following **link**

Directorate for Protection of Personal Data

Status: independent public authority with status as legal entity

Management: The Director and Deputy Director

Responsibility: Before Parliament by submitting an Annual report on the work of the Directorate

Financing: Budget of the Republic of Macedonia and partly own income

Legislation: Directive 95/46/EC on the protection of personal data and the free movement of such data

Convention no.108 on the protection of individuals regarding the automatic processing of personal data by the Council of Europe since 1981

Additional Protocol to the Convention regarding supervisory authorities and cross border transfer of data

Law on Personal Data Protection ("Official Gazette of the RM no. 7/05, 103/08, 124/10 and 135/11)

CAN WE REALLY PROTECT OURSELVES?!

Author: Liljana Pecova-Ilieska, M.A.

The public was highly upset when it appeared PRISM, a secret program of mass electronic monitoring of data managed by the National Security Agency (NSA) of the United States. PRISM is actually code name for the program which collects data that is stored online communications, based on searches made on the internet companies such as Google. There are no indications as to how the data is processed, after being "hacked" and analyzed and what control mechanisms are designed to protect the new location. What is more clear is that the debate about PRISM and the questions that were asked, certainly did not answer the most important: the issue of privacy and confidentiality and protection of personal data.

In this direction was the **statement of Viviane Reding**, the Vice President of the European Commission and EU Commissioner for Justice, given on 14 June 2013 , the debate about PRISM can affect negotiations for EU -US "Free Trade Agreement". She said: "[For] to be successful contract negotiations for trade [...] , there should be trust, transparency and clarity among the negotiating partners. Hereby excludes spying on EU institutions." At the moment when the **Working Party of Article 29 sent a letter** and reacted to these developments expressing strong concerns regarding the violation of basic human rights and the protection of personal data, it's obvious that it was necessary to advance the reforms in EU and the debate intensified in the previous period in the European Parliament need to contribute to the rapid adoption of proposals for change in the area of data protection in the private and public sector as a necessary step and priority for defense against programs such as PRISM.

Given in mind the rapid development of new technologies as a first step towards increasing the misuse of personal data, the Directorate for Personal Data Protection of the Republic of Macedonia has recognized the need to increase public awareness and changing the perception of citizens about their right to protection privacy. Given the recent developments, as well as a survey research made, it came clear that many people that use the Internet and social networks, i.e. 80% of them had low awareness of the procedure for application for abuse of personal data. Therefore a Communication Strategy document was created where influential groups in society were defined (academics, teachers, journalists, mayors, etc.), that will create a positive opinion and educate to increase awareness of the right to protection of personal data. In order to establish ongoing communication that will create public awareness in the field of protection of personal data, and in order to achieve recognition of the identity and work of the Directorate for Personal Data Protection, it was necessary to recognize the idea and intention through exercise in cooperation with several partners, initiatives and organizations. In cooperation with the Embassy of Croatia in the Republic of Macedonia the Communication Strategy document found its space for realization.

In this regard, the Ambassador of Croatia in the Republic of Macedonia, H.E. Zlatko Kramarić, recognized the positive message and purpose of the activities and expressed full support and strong will stating: "the Big Brother" (George Orwell) who sees everything, is not literary fiction at all, this is our rough (and only!) reality. All our movements, all our privacy, our world of intimacy, our ordinary conversations, benign exchanges of our deepest and most sincere emotions, are not just our movements, our conversations, our little secret, but we already share with someone "omniscient view", "curious ears!" And what is most tragic is that we are aware of it, but it does not excite us too much, we actually glossy fit into this Orwell's project of living! It is because of these reasons it is important to give support to any initiative, especially institutional ones that will regulate this (also very) important part of our lives. Therefore, is extremely important to sensitize the public, especially young people, students, academics, teachers, journalists, "weak" subjects (and today we are all, more or less, "weak subjects") on the issue and to allow the public to begin to speak, to think... just because "regulated community" in which clear division between "private" and "public" can guarantee us our right to privacy/intimacy. Only within the "regulated community" we can practice all universal liberal democratic values: freedom of expression, freedom of speech, right to information, right to other opinion, disagreement and behavior, which in no way interferes with thinking and behavior of others, and only such public may suspend the unbearable "terror of anonymity" that the new technology, the Internet and other social networks through the "backdoor" has introduced into our lives."

At the moment when the European Union is taking on more responsibilities and when the issue about the EU budget raised much discussion in the European family, it seems that when it comes to protection of privacy and personal data, each one of us recognizes the importance and impact the protection of privacy has on overall life. And here it is not brought into question at all the budgetary implications when having changes in legislation, within the EU as on national perspective. Simply, the data protection and privacy as a fundamental human right, is seen as an imperative, a priority in every sense. What remains in doubt is: Shall we make enough to protect ourselves?!

TAIEX workshop on protection of biometric personal data whilst processing

The Directorate for personal data protection, with support from the EU Instrument for Pre-Accession Assistance - TAIEX, on 09.10.2013, in Skopje, organized a "Workshop on protection of biometric personal data during their processing." National experts and experts from Data Protection Authorities from Germany, Ireland, Great Britain and Slovenia discussed the experiences in the application of laws on the protection of personal data in relation to the processing of biometric data, their collection for security purposes and issuance of license for processing of biometric data.

Opinions from WP Article 29 here:

Employee's private emails used as evidence to dismiss

On June 19, 2013, the French Court of Cassation ruled in favor of a company for having dismissed one of its employee's (M. X) on the grounds that he was involved in unfair competition. M. X's wrong-doing was based on email exchanges between him and a competitor that were found on his computer's hard drive and used against him as evidence in court. M. X argued that this evidence was inadmissible because it was unlawfully obtained by the company in violation of his right to privacy and to the secrecy of correspondence. M.X claimed that the emails were private and that the company had made a copy of his computer's hard drive without informing him and not in his presence.

The French Court of Cassation ruled in a landmark decision (the 2001 "Nikon case") that "an employee has the right to the respect of his private life – including the right to the secrecy of correspondence – on the work premises and during working hours". Since then, the Court of Cassation has refined its position and progressively balanced the right to privacy of employees against the right of employers to monitor the activities of their employees. Unless marked by the employee as "private", the documents and files created by an employee on a company-computer for work purposes are presumed to be professional, which means that the company can access those documents and files without the employee's presence. However, an employer cannot access files marked "private" stored on the hard drive of a company-owned computer without the employee's presence or informing the employee, unless there is a particular risk or event for the company. It is also presumed that employees use the company's emailing system for professional purposes. Thus, an employer can access an employee's email inbox without his/her presence, with the exception of those that are marked "private" in their subject line, or that are stored in a sub-folder of the inbox named "private" or "personal".

In the given case, M.X challenged the validity of the emails used against him in court on the grounds that those emails originated from his private email inbox, which he had transferred and stored onto his work computer. M.X argued that the company had captured those emails without informing him and that a copy of the hard drive was made in his absence. But for the Court of Cassation, the simple fact that documents or emails, stored on the hard drive of a company-owned computer, originate initially from an employee's private email inbox does not render those emails private. What really matters is whether there is a clear indication that this email is private, such as the word "private" appearing in the subject line, or the fact that it is stored in a folder marked "private".

Since the 2001 Nikon case, the Court of Cassation has made a continuous effort to refine and, in some circumstances, narrow the scope of the right to privacy in the workplace with a view to reaching a fair and balanced approach to privacy in the employment context. Following this ruling, employees should be cautious when storing private emails or documents onto their work computers as they will automatically be considered professional, unless there is an unambiguous indication that they are private. Thus, the risk is high that employees may get dismissed when suspected of unlawful actions because their employer has extensive powers to access all the data stored on their work computer and to use any potentially incriminating information as evidence against them. Simultaneously, employers have an obligation under privacy and labor laws to inform employees about the collection and use of their personal data. This decision illustrates the importance of drafting clear and unequivocal privacy policies explaining to employees how to use the IT equipment and devices that the company puts at their disposal in accordance with the company's internal rules, and how to protect their private data.

Recommendations:

Employees should be cautious when storing private emails or documents onto their work computers as they will automatically be considered professional, unless there is an unambiguous indication that they are private.

At the same time, employers are required by privacy laws and labor law to inform employees about the collection and use of their personal data.

The decision of the Court illustrates the importance of drafting clear and unequivocal privacy policies explaining to employees how to use the IT equipment and devices that the company puts at their disposal in accordance with the company's internal rules, and how to protect their private data.

Please tell me what to do, given that a fake profile on Facebook was created, on my behalf, where my personal data and pictures are abused. In addition I am sending you the fake account link and a link to my personal FB profile.

Dear Madam/Sir,

Regarding your question, please be informed that the Directorate for Personal Data Protection, acts only on requests to delete fake profiles of people whose personal data in social networks are misused by third parties. Also, if you want to delete the disputed account, you need to provide additional documentation to the Directorate for Protection of Personal Data, which is available at the following link

Can you please tell me the following information: Up till 2008 I was using the services of one bank, i.e. had a bank account that my salary was transferred to from the company where I worked. In 2009 I switched to another bank and credit cards used I returned to restore and pay the amount of these debts. However , in order to return the cards back I was asked to fill out a form to update my personal information. I am interested in :

- Do I have a legal right/ability to request deletion of my personal data from the records of the first bank whose user I was?
- Do I have a legal right to refuse an update my personal information at times when I want to eliminate the slightest connection with that bank?
- Based on what is asked of me to update my personal information?

Dear Madam/Sir,

Please note that in accordance with Article 5, paragraph 1, lines 1,2, and 4 of the "Law on Personal Data Protection of the Republic of Macedonia", personal data are processed fairly and in accordance with law, and shall be collected for specific, clear and legally defined purposes and in a manner that is consistent with those goals. Data should be accurate, complete updated, taking into account the purposes for which they are collected or processed.

In accordance with the "Law on Prevention of Money Laundering and Other Proceeds from Crime and Financing of Terrorism" ("Official Gazette of RM 4/08 , 57/10 , 35/11 and 44/12) , i.e. Article 27, the data on the client who has signed a long-term business relationship agreement in terms of the law are kept for at least ten years from the date of termination of the business relationship. When the client is an individual, his identity is identified by submitting an original and valid document, banks must retain a copy thereof. Hence, the Directorate informs you that the officials in the bank acted in accordance with the legislation in Macedonia. In this particular case it is about the exercise of legally determined rights or obligations of the data subject or controller.

Your questions/dilemma you can send to:
info@dzlp.mk

Request for confirming violation of the right of personal data protection

Download HERE

Twitter surrenders anti-Semitic tweet info to French authorities

The company had resisted for months, but finally relents, hoping to "put an end to the dispute" and saying it will do its part to "fight racism and anti-Semitism." Twitter has finally released data on anti-Semitic tweets to French authorities. The company said in a statement obtained by the AFP on Friday that it has complied with a French government request to hand over tweets related to a rash of anti-Semitism on the site. Last October, several anti-Semitic tweets and hash tags appeared on Twitter, including the objectionable "#UnBonJuif est un juif mort," translated as "A good Jew is a dead Jew." Twitter took the offending tweets off its site after the Union of Jewish French Students (UEJF) and other anti-racism groups requested takedowns.

But the case wasn't over there. The UEJF in January won a court ruling compelling Twitter to hand over the names of those who had posted the anti-Semitic remarks. Two months later, the UEJF sued Twitter for $50 million, alleging that the company did not comply with the court's request. Last month, an appeals court ruled Twitter must provide the groups and authorities with the names of those who posted the offending tweets

For its part, Twitter said that it was "disappointed" that it was being requested to turn the data over, and was considering filing another appeal. Today, however, Twitter changed its tune, saying that it has provided data to authorities that would enable "the identification of some authors." Twitter said in a statement that the decision to hand over the data will "put an end to the dispute," adding that it will work with the UEJF to "fight racism and anti -Semitism."

Opera MINI brings privacy mode to basic mobile browser

Just because it's not a smartphone doesn't mean it's dumb. Norway's Opera is bringing increasingly advanced functionality to its most low-end Mini browser, with version 4.5 boasting a privacy mode and download manager.

On Wednesday morning, the Norwegian software firm brought out a new version of the browser's low-end iteration, Opera Mini 4.5. This is intended for basic Java-capable phones – those with beefier phones that still fall short of "smartphone" status can download a more functional version, Opera Mini 7.5. One of the standout features of Mini 4.5 is a new privacy mode – bear in mind that it's little over a year since Google brought Chrome to Android, incognito mode and all. In keeping with the intended markets, Opera is pitching this as ideal for sharing your phone with friends who can then check their Facebook without any logins or data being saved. he browser now features a download manager that allows the user to pause, resume and manage downloads (this was previously available on Opera Mini 7.1, but not on the basic version). It has also been given a general refresh, both visually and in terms of footprint (it is now lighter), and boasts new touch enhancements such as kinetic scrolling for touch-capable phones. As Opera Mini product manager Christian Uribe noted in a statement, we're seeing features gradually trickle down from the recently overhauled smartphone version of Opera down to the lightest-weight version. "Having an excellent download manager is just as important for the students downloading class work to their phones as it is for business people with more advanced phones," Uribe said. Add to this the fact that (as with all Opera browsers) Mini 4.5 users get to use data compression technology that can cut costs by up to 90 percent, and it becomes clear that the low end of the mobile business is nowhere near as dumb as it used to be. Which is just as well — for many of the intended users, these basic phones are effectively their personal computers.

Contact:

Directorate for protection of personal data

Blvd. Goce Delcev 18

1000 Skopje, Macedonia

tel: ++389 (0)2 3230 635

fax: ++389 (0)2 3230 635

E-mail:

info@dzlp.mk

info@privacy.mk

web:

www.dzlp.mk