**Requirements to comply with the new data privacy law in Russia**

1. **Summary – three main principles of personal data localization:**

* All information related to the individual, which allows to identify her/him, is in scope unless there is only ONE element of personal data at hand – for example, first+last name, OR email address, OR phone number etc. Any combination of two or more such elements brings all the data within the scope of localization obligations.
* Only “primary” databases are subject to localization, that is, only those where the data is sent to, recorded or updated by the individual (“subject” of personal data) her/himself. “Secondary” databases, whereto the data is extracted from other IBM databases, are not subject to localization.
* Only the data collected directly from the individual is subject to localization (i.e. which is sent, recorded or updated by the individual whom this data pertains to, or on her/his behalf). For example, contact data will be subject to localization (in a primary database as above) irrespective whether the individual or her/his assistant submits it into a system. However, salary data submitted into the system directly by IBM Payroll, is not subject to localization, because it is not collected by IBM Payroll from the individual.

Please see below for more details.

1. **Description of the Legal Framework**

Russia introduced a **data privacy law amendment requiring that personal data of Russian citizens should be stored and processed in Russia**.

The new law says exactly the following:

*“During collection of personal data, including via the ‘internet’, the personal data operator must ensure that recording, systematization, accumulation, storage, adjustment (updating, alteration), retrieval of personal data of Russian citizens is performed using the databases which are located on the territory of Russian Federation”.*

The law will be effectiveas of **September 1, 2015**.

Key definitions:

***Personal data*** – *any information which directly or indirectly relates to an identified or identifiable individual.*

There is no exhaustive list of what personal data is, but it will include the usual suspects (name, address, phone numbers, passport information and the like). The current position of the regulator is that just one element (for example: first+last name, OR just the email address, OR just the phone number) will not constitute personal data for the purposes of the law (since in most cases it does not allow to identify a specific individual) while a combination of at least two of such elements will.

***Data Operator*** – *an entity or individual who collects and processes the personal data and defines the purposes of collection and storage*.

The concept of a “data operator” in Russian law is very close to the EU concept of “controller”. In the 1995 Data Privacy Directive, a controller is “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

***Collection of Personal Data:*** This concept is critical for the localization requirement, because only such data must be localized by the Operator which is “collected” by it.

The law does not provide the definition of “collection”, thus there may be various interpretations. According to the narrow interpretation, the data is “collected” only where an operator is getting personal data directly from the data subject (the person to whom this data pertains). Another possible (broader) interpretation of collection includes situations where personal data comes to a company from any other sources. However, there are arguments in favor of the former, narrow interpretation.

First, article 18.1 of the current Personal Data Law conditions the collection upon certain actions of an operator, which would normally be performed only during interactions with data subjects (e.g. informing them about the purposes of collection, etc.). Such actions will be quite difficult to perform if the collection is performed not from the data subjects.

Second, the CIS model personal data act adopted in 1999 by the inter-parliamentary assembly of the CIS, contains a clear definition that collection is obtaining personal data from the subjects of such data. Although this model act is not a valid law in Russia, it can be used as a persuasive authority (or “soft law”) helping understand the concepts of a valid law, in the absence of the explanation of these concepts in the valid law itself.

Based on the above, the narrower interpretation could be accepted in certain cases. As this area is still grey, certain organizational/procedural changes may be required in addition, which will **not change technical aspects** though. For example, requiring the IBM counterparts to confirm, in some way, that they have “collected” and localized the data themselves.

***Database*** *– for the purposes of the law means any organized file of information, regardless of media type, tools, or methods of processing (e.g. a Word file, an Excel spreadsheet, or even card files with personal data).*

**According to the new data privacy legislation IBM has to ensure that:**

1. **Personal data of Russian citizens collected by IBM should be processed and updated *using only the databases located on the territory of Russian Federation.***
2. **In other words, a master record of this data must be stored in a database located within Russia, and only after that, it can be transferred to databases located abroad in accordance with provisions on trans-border transfer of personal data. The same applies to the updates and additions to the personal data contained in such databases.**

**Key clarification statements (see sections 3.2-3.3 for details):**

* The database where the data is initially recorded into, as well as stored and updated at a later stage, must be located in Russia (the “primary database”). Copies (“secondary databases”) of such “primary databases” can be transferred outside of Russia.
* Based on the above, IBM’s current interpretation is that IBM non-Russian (“secondary”) databases containing exactly the same information as already contained in a local/localized “primary” database, are not subject to localization. There are arguments in favor of this interpretation, but it cannot be excluded that the regulator may take a different position at a later stage. This question was raised in discussions with the regulator in spring 2015, but the regulator did not explicitly confirm, nor reject this interpretation.
* Although the law text is silent on this, the regulators explained that in their view, such solutions where the primary database which the data is collected into, remains abroad, and only a Russian replica of such foreign database is created, – contradict to the law. The regulator stated that the primary database must be in Russia, while replicas abroad are not prohibited.
* The law applies not only to collection of personal data via the internet, but also to any other collection of personal data (e.g. manual, non-computerized).
* The law applies to all “data operators” if they conduct activities in Russia. Although this is not stated in the law, according to the current understanding the law covers personal data of Russian citizens collected in the territory of Russia only, even if collected by foreign “data operators” who target their activities to the territory of Russian Federation (for example, via a Russian version of their Internet services)
* Although the law itself is silent on this, the current interpretation of the regulator is that the law does not apply to “data operators” collecting personal data of Russian citizens who live outside of Russia.
* Systems of personal data collection which IBM has access to, but which are owned and operated by third parties, are out of IBM localization obligation’s scope, provided that such a third party has the prevailing role in running the system and determining the purposes of the data collection and processing. This is not stated explicitly in any law or regulation, but is IBM’s current interpretation based on several corresponding legal provisions. It cannot be excluded though, that the regulator takes a different position at a later stage.
* Systems storing and processing personal data objectively coming not from the data subjects (individuals) directly, but from other entities (for example IBM’s business partners, customers or suppliers) are out of scope if IBM receives an affirmative confirmation from the companies in question that the data entered into the tools has been earlier collected and localized according to the law. This is not stated explicitly in any law or regulation, but is IBM’s current interpretation based on several corresponding legal provisions. It cannot be excluded though, that the regulator may take a different position at a later stage. This question was raised in discussions with the regulator in spring 2015, but the regulator did not clearly confirm, nor reject this interpretation.
* Such non-Russian databases into which the main personal data (basic individual information) comes from Russian local “primary” databases, are also subject to localization, IF additional data “allowing to identify the individual” (for example, travel expenses, skills etc.) is added directly to such databases.

**Technical solutions for global systems/databases:**

Solution 1.1 - Create a custom Local Application & DB and integrate them with the Core Application & DB as follows: when data is entered and saved in a Local Application & DB and after data is saved locally, it will be automatically transferred into the Core Application & DB. Point of entry – fully local, new application, new interface. This solution will require changes in the Core Application and development of the Local Application User interface & DB and requires bi-directional synchronization between them.

*Legal comment: This solution is the most compatible with the purpose of the law and the current regulator’s interpretation, thus the preferred one.*

Solution 1.2 – Create a custom Local Application & DB and integrate them with a Core Application & DB as follows: when data is entered into the Core Application (via core application user interface), it will be saved in a Local DB and in the Core DB simultaneously (in online mode).. In other words, there is an application/interface hosted outside of Russia, and two databases – one in Russia and one outside of Russia. The data entered through the application/interface is saved directly from the application to two databases – foreign and local – in parallel.This solution will require changes in the Core Application and development of the Local Application and DB.

*Legal comment: This solution seems to comply with the principle explained by the regulator – that the actions with personal data, such as input/recording and updating, must be taken in the Russian database in the first instance. However, the concern may be that the interface is still foreign (hosted abroad) and thus it cannot be excluded that it records some information directly in some foreign database. According to the current interpretation of the authorities, the idea of the law is that the control over personal data must be in Russia. By using a foreign interface, we are taking one step in departing from this principle. Therefore, this solution is not the preferred one – but at the same time not totally impossible.*

Solution 1.3 – Create a Local DB as an instance of the Core DB and configure a real-time replication between Local and Core databases. This solution requires a special replication procedure at the database level for Local and Core DBs. Thus data is entered through a Core Application User Interface and saved into both Local and Core DBs. Application and interface are foreign, primary database is foreign and it simultaneously replicates with the local database. Could be considered as backup solution option in case solutions 1.1 or 1.2 are not possible.

*Legal comment: The previous comment equally applies here, but the concern is even stronger. If one questions which database is “primary” here – Russian or foreign – the answer is either “this is not clear, they are synchronized in real time” or “foreign”. This is derogating even stronger from the regulator’s interpretation, thus may be considered only if the previous two turn out to be totally impracticable, which needs to be properly documented and risk accepted.*

Solution 1.4 – Create a custom Local Application & DB and change the local business process as follows: data is first entered in Local Application & DB, and after that, data is re-entered manually into the Core Application. 1.4. is a backup solution which entails certain risk, thus it shall be considered only if options 1.1, 1.2 or 1.3 are not possible)

**Technical solutions for systems/databases used only by Russian entities but hosted abroad:**

Solution 2 – Fully migrate Core Application and Databases to infrastructure located in Russia.

**Organizational solutions for global systems/databases:**

Solution 3.1 – For those personal data which is coming not directly from the individual, but from third party legal entities, get a confirmation from these legal entities that they themselves collect and localize this personal data in due course. These entities have their own responsibility concerning personal data localization.

Solution 3.2 – Change the local process as follows: the data (files) are first received via e-mail and then they are manually saved in a local Lotus Notes Team Room and only after being saved locally the data are manually re-entered into a global Core Application. A special role will need to be created for entry of personal data into the Core Application.

Solution 3.3 – Change local process as follows: establish an internal IBM rule stating that it is not allowed to enter personal data to a global Core application. Ideally make changes into application in order to block / hide corresponding functionality.

1. **List of applications in scope:**

*Legend of priority levels:*

H – high: needs to be resolved in priority mode and controlled on daily basis.

M – medium: requires attention and resolution, however H shall take priority over M in case for some reason they cannot be handled with the same level of urgency.

L – low: requires attention and resolution only following the resolution of H and M.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Application name | Personal data held | Proposed Solution | Priority |
|  | Domain: Corporate business applications | | |  |
| **1** | **HRMS** | Employee basic personal data, salary, contact data etc. | **1.1 is preferred. 1.2 (and following it, 1.3) may be considered if 1.1 turns out to be totally impracticable, which has to be properly documented and the risk accepted.** | **H** |
| **2** | **DRMS** | Outstaffing agencies’ employees name | **3.1** | **M** |
| **3** | **GOM** (third party system) | Candidate basic personal data, education, experience, contact data | **3.2 + negotiate with NetMedia regarding localization of their database** | **M** |
| **4** | **Kenexa** (to be deployed in Russia in Oct/Nov 2015) | Candidate basic personal data, education, experience, contact data | **1.1 is preferred. 1.2 (and following it, 1.3) may be considered if 1.1 turns out to be totally impracticable, which has to be properly documented and the risk accepted.** | **H** |
| **5** | **HR RUSSIA DB (HR Lotus Notes** **teamroom)** | Employee basic personal data, salary, contact data | **2** | **H** |
| **6** | **IBM Ru Insurance DB** | Employee basic personal data, contact data | **2** | **H** |
| **7** | **Server with scanned travel documents** (not deployed yet) | Employee basic personal data, personal id number | **2** | **H** |
| **8** | **WWER, TSOB1** (Travel Server) | Employee basic personal data, travel expense data | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2. Solution 3.2 may also be considered in parallel.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **M** |
| **9** | **Expertise assessment tool** | Employee basic personal data, skills, experience, contact data | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2. Solution 3.2 may also be considered in parallel.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **M** |
| **10** | **PBC tool** (personal business commitments) | Employee basic personal data, personal targets and rating (feedback on work results) | **To be reconsidered after resolution of H and M** | **L** |
| **11** | **LMS** (learning) | Employee basic personal data, online trainings accomplished | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **L** |
|  | Domain: Services | | |  |
| **12** | **ILC** (labor claiming) | Employee basic personal data, working time spent for particular project | **To be reconsidered after resolution of H and M** | **L** |
|  | Domain: Digital channel | | |  |
| **13** | **Lotus Notes mail** | Employee contact data, emails | **In case Notes mail will be migrated to SmartCloud Notes by the end of 2015 there is no sense to buy and set up appropriate infrastructure for Notes just for 3-4 months. Focus should be put**  **on Verse mail.**  **In case the schedule of Notes migration will be delayed this decision has to be reconsidered.** | **L** |
| **14** | **SmartCloud Notes / Verse** (not deployed yet) | Employee contact data, emails | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **H** |
| **15** | **IBM ID** (web id) | Employee basic personal data, contact data | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **H** |
| **16** | **w3 Connections[[1]](#footnote-1)** | Employee basic personal data, report chain, network, posts/blogs | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2. Solution 3.3 may also be considered in parallel.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **M** |
| **17** | **Connections social cloud** | Employee and external users basic personal data, posts, contact data  External individuals employee basic data, posts, contact data | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **H** |
| **18** | **ibm.com Connections** | Employee and external users basic personal data, external user basic personal data, contact data, background info, posts | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **H** |
| **19** | **ibm bluepages** | Employee basic personal data, contact data, skills, experience | **To be reconsidered after resolution of H and M Alexey A: In fact, I would recommend a solution preventing the employees to enter additional data into this application** | **M** |
|  | Domain: Marketing, Sales & Software Fullfillment | | |  |
| **20** | **SalesConnect / Global partner portal** | Potential or existing customer employee basic data, contact data | **1.1 is preferred. 1.2 (and following it, 1.3) may be considered if 1.1 turns out to be totally impracticable, which has to be properly documented and the risk accepted. 3.2 may also be considered in parallel.** | **H** |
| **21** | **Passport advantage** | Existing customer employee basic data, contact data. Data filled in externally | **3.1 . Process shall be changed to prevent direct registration for open distribution** | **H** |
| **22** | **IBM PDL** | Existing customer employee basic data, contact data. Data filled in internally | **3.1 (together with Passport advantage application)** | **H** |
| **23** | **GRP** | Marketing events attendees basic data, contact data | **1.1 is preferred. 1.2 (and following it, 1.3) may be considered if 1.1 turns out to be totally impracticable, which has to be properly documented and the risk accepted.** | **H** |
| **24** | **EIT (Event Import Tool)** | Marketing events attendees basic data, contact data | **3.1, 3.2** | **M** |
| **25** | **PartnerWorld Portal** | Partner employee basic data, contact data | **3.1 The process shall be changed similarly to the PA, see 21.** | **H** |
| **26** | **C2S2** | Partner employee basic data, contact data | **3.1** (together with PartnerWorld) | **H** |
| **27** | **Lotus Notes team room with Partners' data** | Partner employee basic data, contact data | **3.1** (together with PartnerWorld) | **H** |
| **28** | **Software access catalog** | Partner employee basic data, contact data | **3.1** (together with PartnerWorld) | **H** |
| **29** | **Marketing RU teamrooms** (IMC EEA Event, Doclib RCIS) | Marketing events attendees basic data, contact data | **2** | **M** |
| **30** | **IWM** (ibm web membership) | Marketing events attendees basic data, contact data | **1.1 is technically not feasible (see justification after the table)**  **Preferable solution is 1.2. Solution 3.3 may be also considered in parallel.**  **1.3 may be considered if other solutions turn out to be totally impracticable, which has to be properly documented and the risk accepted** | **H** |
| **31** | **Marketing tools for invitation of customers to IBM events (via ibm connections, lotus notes databases and teamrooms)** | Existing customer employee basic data, contact data | **3.2** | **L** |
|  | Domain: Systems and supply chain | | |  |
| **32** | **SOF** | Potential or current customer employee basic data, contact data | **1.1 is preferred. 1.2 (and following it, 1.3) may be considered if 1.1 turns out to be totally impracticable, which has to be properly documented and the risk accepted. 3.2 may also be considered in parallel.** | **H** |
| **33** | **CSA (Contractor Sourcing Application)**  **BOND (Buy on Demand)**  **CAAPS (Common Alternative Accounts Payable System)**  **Content Manager, CAAPIT**  **PBC (Procurement Business Control)**  **ECM (Emptoris Contract Manager)**  **SFT (Source File Tool)**  **GCDS (Global Common Document Store) RT (Req Tracker)**  **SDDB (Global Support Desk DB)** | Supplier employee basic data, contact data [whose contact data?] | **3.1 [only provided that it is feasible to get such confirmations, depending on what kind of contact data there is]** | **L** |
| **34** | **Other Russian Lotus Notes teamrooms** | Various data depending on purpose of each teamroom | **3.3** | **L** |

\* Solution 1.1 could NOT be considered for applications: WWER, Expertise assessment tool, LMS, Verse, IBM ID, w3 Connections, ibm.com Connections, IWM due to:

* These applications use global web-based interface with complex logic. The major part of user interface is used for personal data modification, thus it should be totally reproduced in a local application.
* These applications have a built-in complex integration with other systems (e.g. WWER with Amex system, w3 Connections with HRMS etc.)
* In case local application will be created it will require a complex bi-directional synchronization with the core application. Moreover creation of a local application for replacing collaboration systems, which are used by international teams (like Connections and Verse), seems unrealistic due to its way of using.

As a result, to create a local application which will replace functionality of the global application means to recreate full application functionality and build integration which seems to be unrealistic. The alternative option which could be considered in some cases: to put an instance of the core application onto Russian servers and somehow synchronize it with the global application instance (needs to be discussed with application owners and SMEs).

1. Differences between w3 connections, connections social cloud, ibm.com connections are described here: https://w3-connections.ibm.com/communities/service/html/communityview?communityUuid=511fa0b6-c6cb-44eb-97ac-059fc32ed02c [↑](#footnote-ref-1)