SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

How to protect personal data and comply with regulations

searchinform.com

There is a global trend, regulators tighten the legislation, aimed at data protection. Below is the list of a few, probably, most well recognized regulatory acts:

- PDPL (Indonesia)
- GDPR (EU)
- KVKK (Turkey)
- PIPL (PRC)
- LGDP (Brazil)
- SAMA (Saudi Arabia)
- PDPB (India)
- PDPA (Thailand)
- PERSONAL DATA PROTECTION ACT 2010 (Malaysia)
- Bundesdatenschutzgesetz – BDSG (Germany)

Etc. excluding sector-specific legislation!

Despite the large amount of various regulations, most of them have some same aims: **prevent unauthorized and illicit access to Personal Data, its disclosure, change or inappropriate disposal.**

In order to meet the regulators' requirements, organizations, among other things, must:

- Obtain all the personal data, reveal, where it's kept.
- Define, which users should have rights to work with personal data and prevent cases of illicit access to such data.
- Define the list of resources, which can be used for personal data keeping. Prevent keeping personal data elsewhere (including users' workstations) and detect, if there are any cases of inappropriate data keeping.
- Take preventive measures to ensure safety of the processed data, including users' access rights management (access rights distribution).
- Take all the required measures to ensure safety of personal data keeping, processing and transmitting processes (use only approved data processing technologies, data transmition channels; implement cryptoprotection).
- Analyze information systems' vulnerabilities.
- Detect and analyze any incidents (quite often, it's also required to notify the regulator about the incident and report on the results of the investigation).
- Keep employees up to date in information security related issues and enhance their IS competencies.
- Many acts contain the requirement, known as Right to be forgotten, which enshrines the right to have personal data deleted from Internet searches and other directories.

In this document we'll reveal, how SearchInform helps organizations to comply with basic regulations' requirements.

** according to the 2022 global survey by SearchInform*

How to ensure protection of personal data?

In order to mitigate the risk of data leak incident, it's required to implement information security (IS)-tools:

- **DCAP** class solution obtains all the personal data, kept in the organization's storages; detects any operations on it and appropriately distributes access rights to confidential data.
- **DLP** class solution automatically detects a data leak attempt, prevents the incident and gathers evidence for precise investigation.
- **SIEM** class solution reveals external attacks and other threats, posed to the personal data processing systems; reveals the correlation between security events, which caused the incident.

Let's examine, how to configure rules of personal data protection with the help of FileAuditor, SIEM and DLP solutions by SearchInform.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

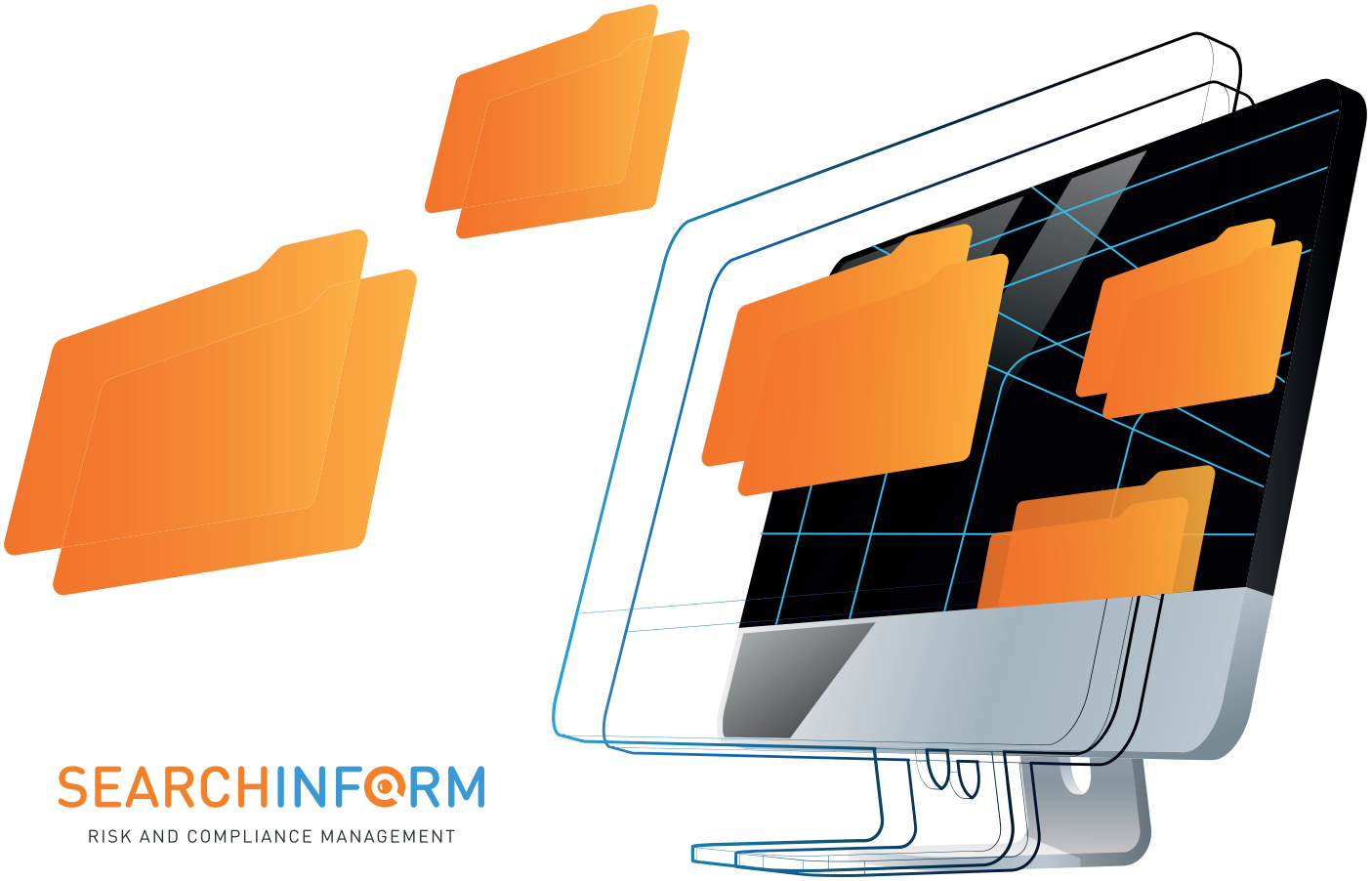
1. Obtaining all the personal data

For example in: **Personal data protection act 2010, Part II, 9 (1) (b)**

First of all it's required to obtain and classify all the files, which contain personal data: passport information, phone numbers, bank card details etc. The **FileAuditor** solution helps to deal with this task.

In order to ensure protection of documents, containing personal data, it's required to configure automated classification rule. FileAuditor provides users with ready-made templates, including aimed at search of files, containing personal data ones. What's more, you can add an unlimited amount of new categories.

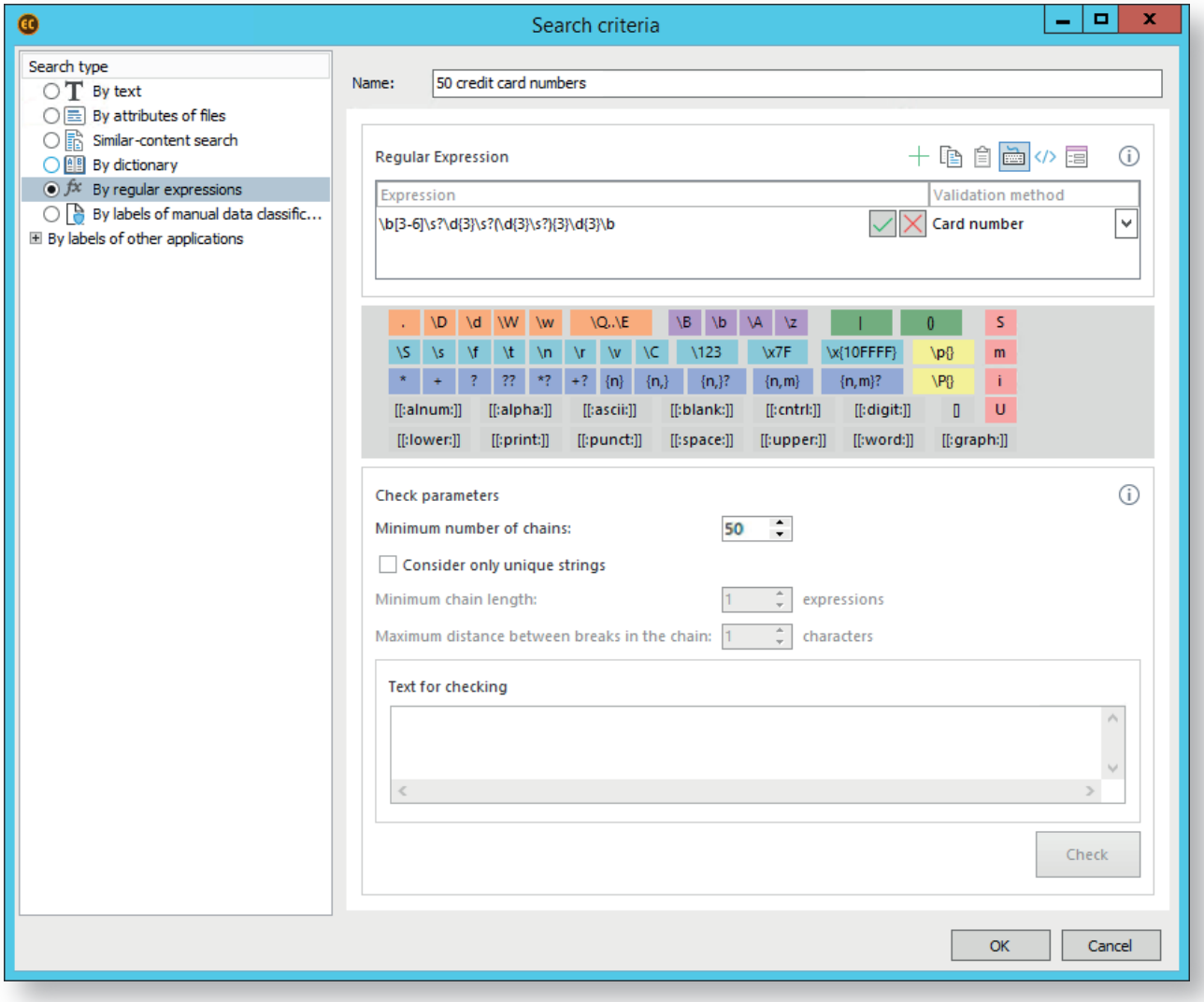
After the configuration of rule in FileAuditor is completed, the solution scans all the directories, where the data is kept and obtains all the required files. The solution adds the label to all the documents, containing personal data, what's more, it ensures control of users' operations on files. For instance, thanks to the FileAuditor, the IS officer knows all the users, who work with such files (e.g. open, edit, delete them). What's more, with the help of FileAuditor the employee in charge knows, who has access to these files. Excessive access rights can be limited as well: the system allows to prohibit reading, editing, resending documents, containing the specified label (in our case, personal data label) in any application. Blockings can be applied for all users or only for the specified ones, as well as they may be applied for some specific workstations solely.



SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

How to configure?

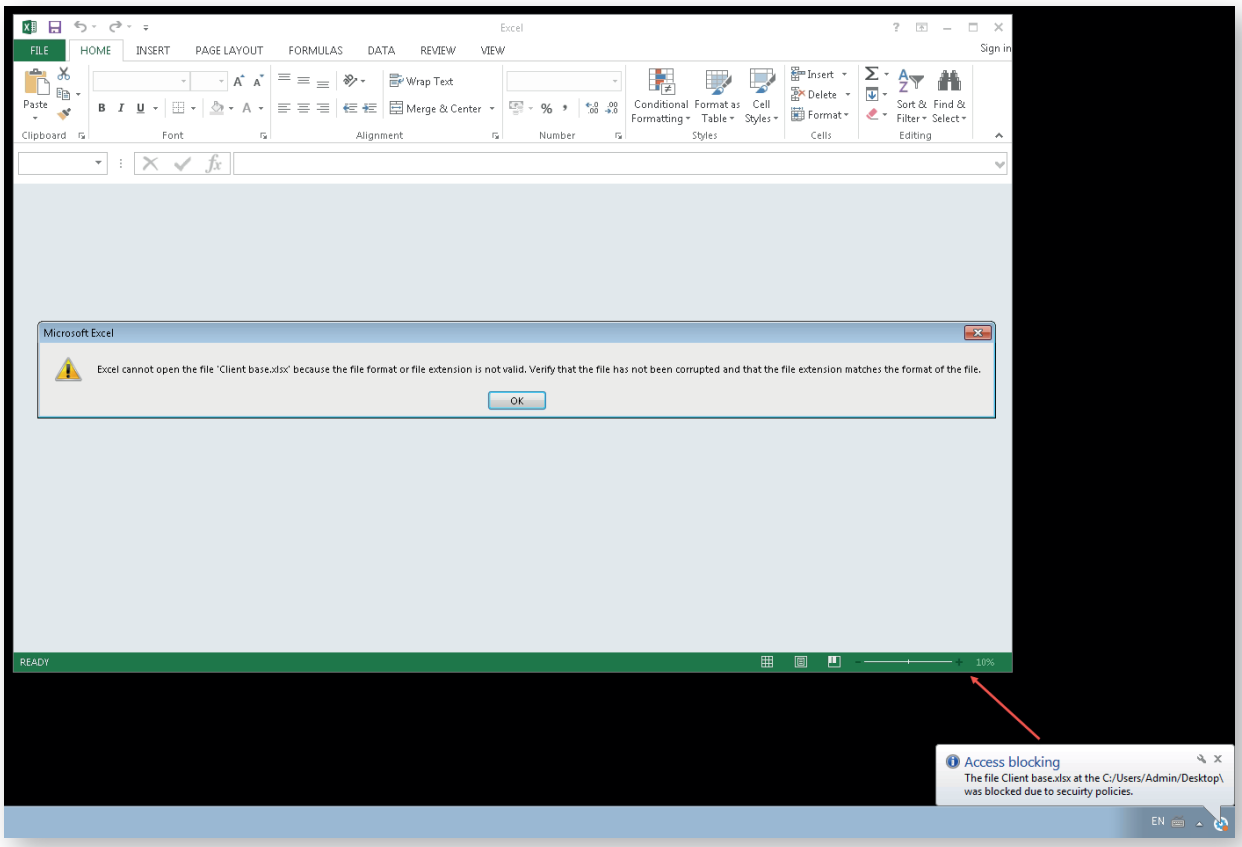
In the FileAuditor settings the pre-configured template for automated search of documents, containing personal data is available. It may be used with the default parameters or fine-tuned according to client's requirements. For instance, you may specify the search criteria to perform search according to the file format. Thus, the system will search for personal data only in files of the specified format, e.g. *.DOCX, *.DOC, *.PPTX, *.RTF, *.XLSX, *.XLS etc.



Setting parameters for bank card search policy

Blockings

You can configure blockings according to the Personal data label: thus, reading in the specified or arbitrarily defined programs, as well as sending via email or any other application will be prohibited. For instance, you can prohibit to open client databases in MS Excel and attach labelled files in Telegram. Blockings are implemented to a file at the level of file attributes, what ensures, that programs simply can't access the files. Thus, there is no chance left for users to perform risky operations with confidential data.



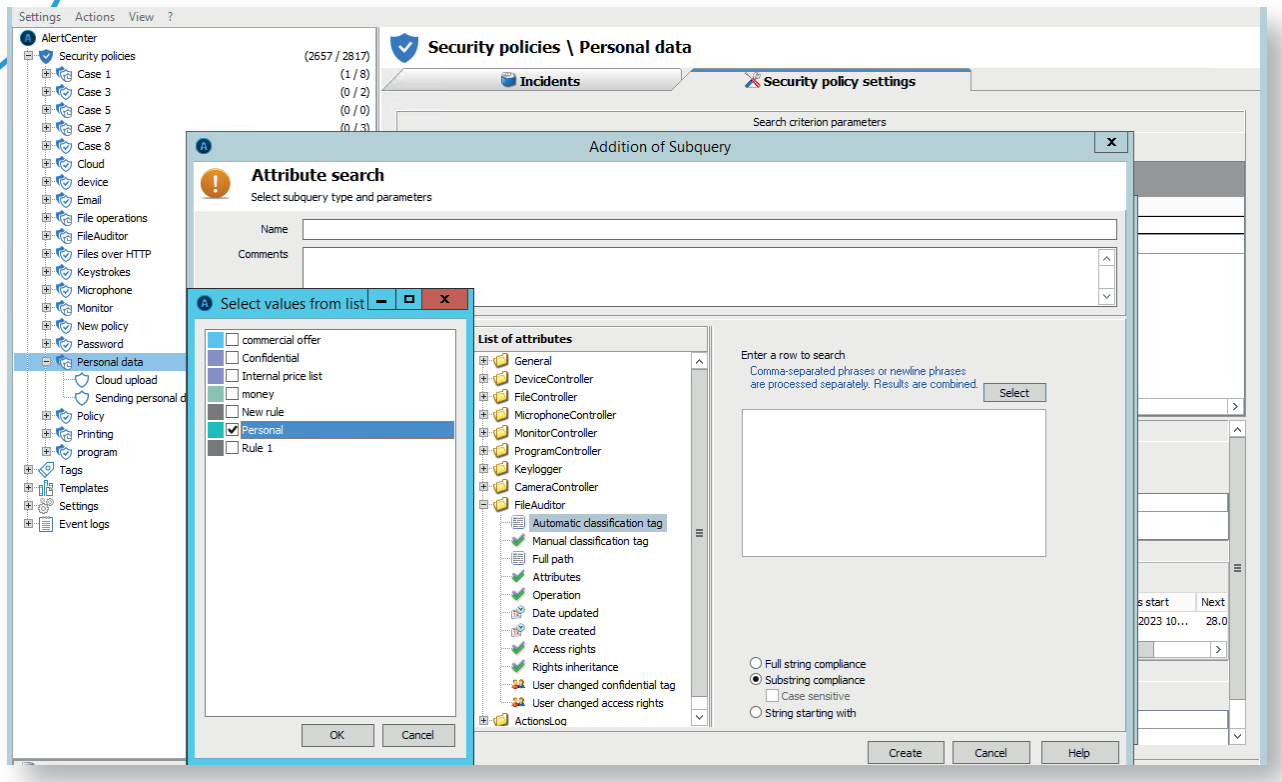
Blocking implementation

2. Ensuring protection of personal data against leaks

For example in: **GDPR Art. 5, 1 (f)**

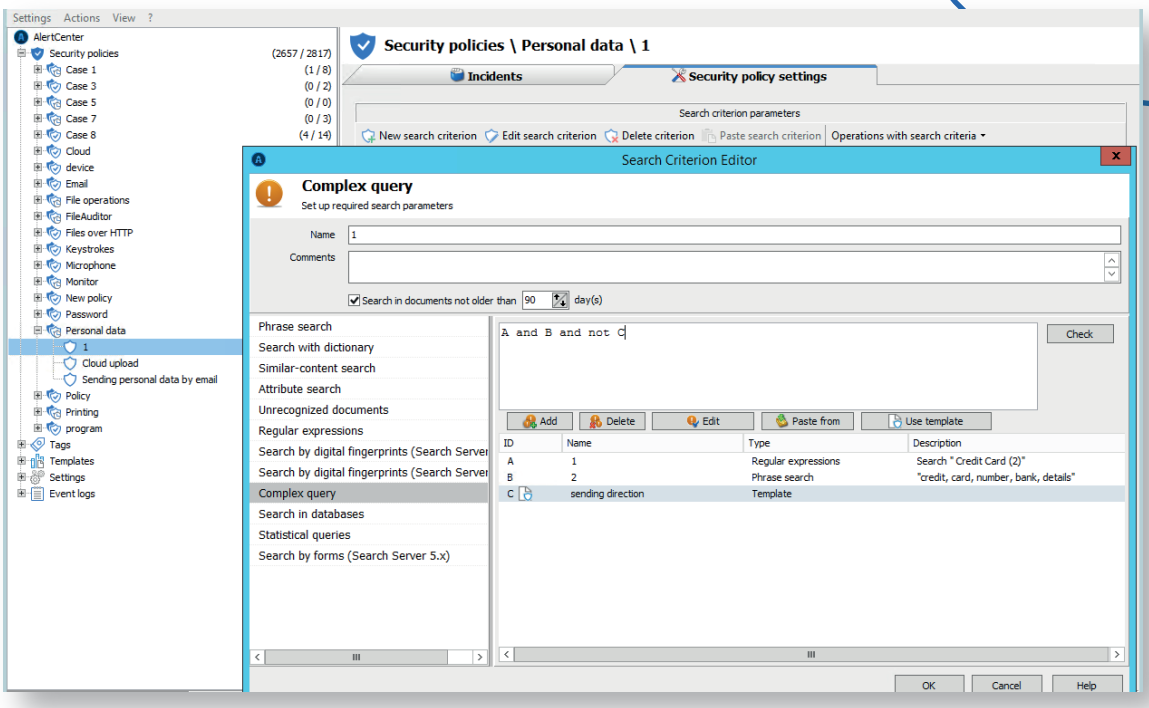
At the next stage it's required to make sure, that all the personal data obtained won't leave the corporate perimeter. This can be ensured with the help of the DLP system.

SearchInform DLP performs analysis of all the data array and in case a violation of personal data processing is detected, immediately notifies an IS officer about the incident.



Configuring criteria for search according to FileAuditor labels

SearchInform DLP provides a set of preconfigured Personal data policies: they control transmission of bank card numbers, phone numbers, passports and other personal details to third parties. Policies contain a few search criteria, for example, in order to protect payment details the following ones are implemented: search for card numbers via search by regular expressions; search of the card word via search by phrases; data template, containing information on data transmition (whether it was sent from or to the corporate email). The policy ensures control of card details sending via different sources – messengers, email, Skype etc., depending on the installed DLP interception modules.



An example of pre-set Personal data group policy

In order to prevent data leaks, the DLP by SearchInform, just like the FileAuditor, enables to block operations of personal data sending – it doesn't matter, whether, personal data is contained in a file or in a text message. The restrictions are applied to email, web-resources, messengers, flashdrives, remote connections, printers, FTP-connections and any other channels, controlled by the DLP system. Blockings are content-based and when they are implemented, the system considers various other attributes as well: for instance, file, PC and user name; recipient's email address; file size and format etc.

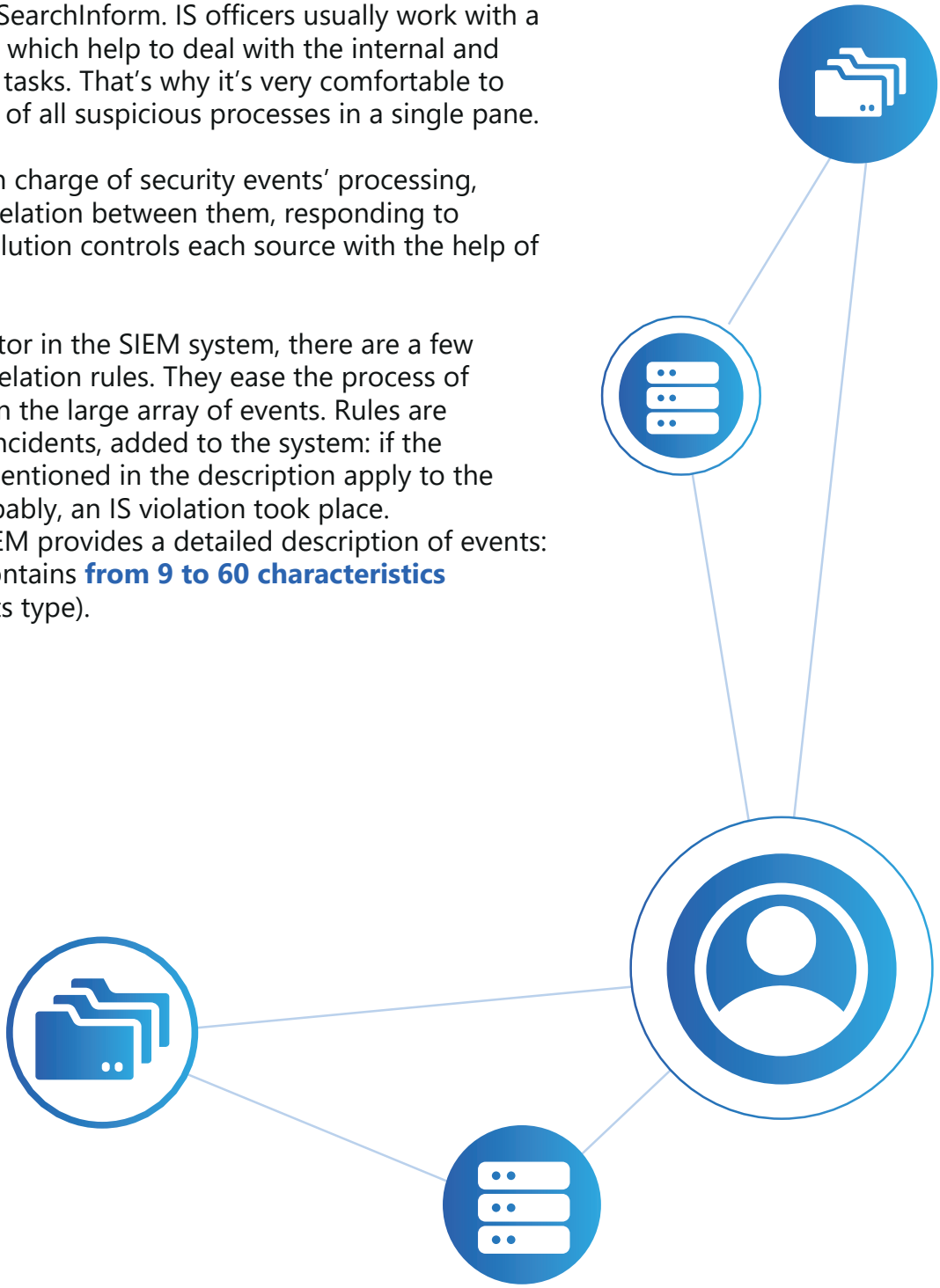
What's more, the DLP solution provides the detailed incident map. When conducting an investigation, it's possible to find out, what a user did before he/she attempted to leak personal data; with whom did the user communicate; reveal the motive behind the user's action: whether it was an accidental data leak, case of industrial espionage or something else.

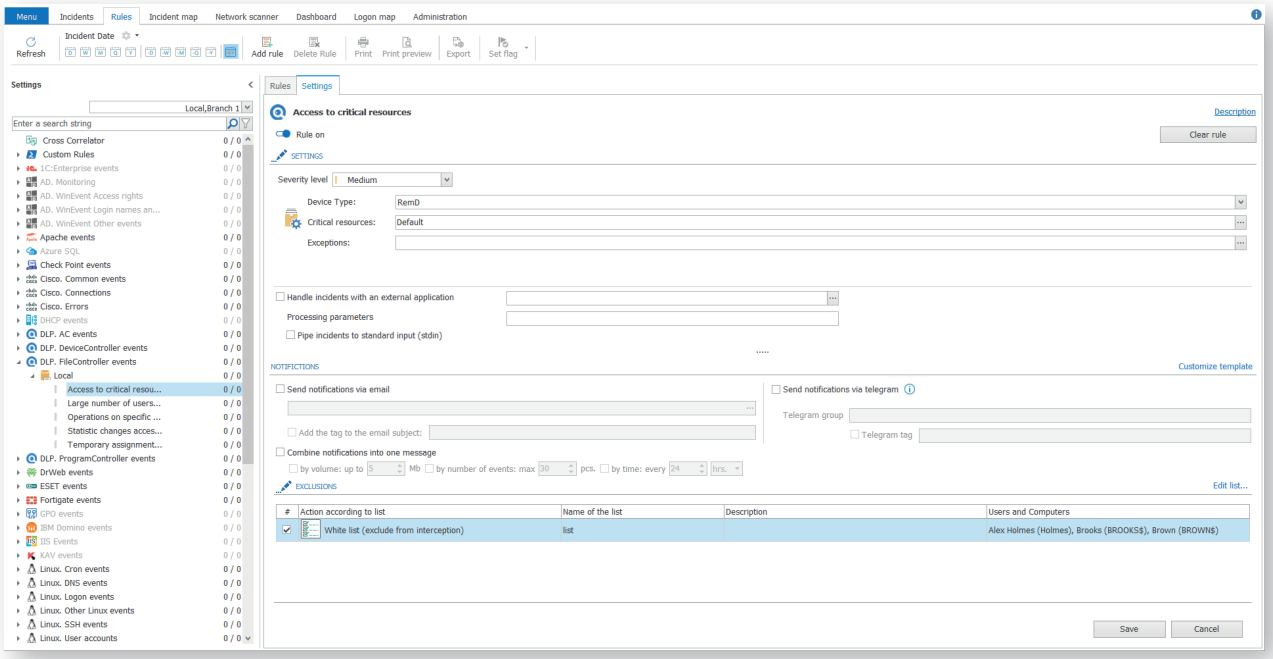
3. Mitigation of other threats, posed for personal data

All the incidents, which are detected by DLP and DCAP systems can be gathered and examined with the help of the SIEM system by SearchInform. IS officers usually work with a number of tools, which help to deal with the internal and external security tasks. That's why it's very comfortable to perform analysis of all suspicious processes in a single pane.

SIEM system is in charge of security events' processing, establishing correlation between them, responding to incidents. The solution controls each source with the help of a connector.

For each connector in the SIEM system, there are a few pre-defined correlation rules. They ease the process of incident search in the large array of events. Rules are descriptions of incidents, added to the system: if the characteristics mentioned in the description apply to the event, most probably, an IS violation took place. SearchInform SIEM provides a detailed description of events: a single event contains **from 9 to 60 characteristics** (depending on its type).





Configuring AlertCenter rules

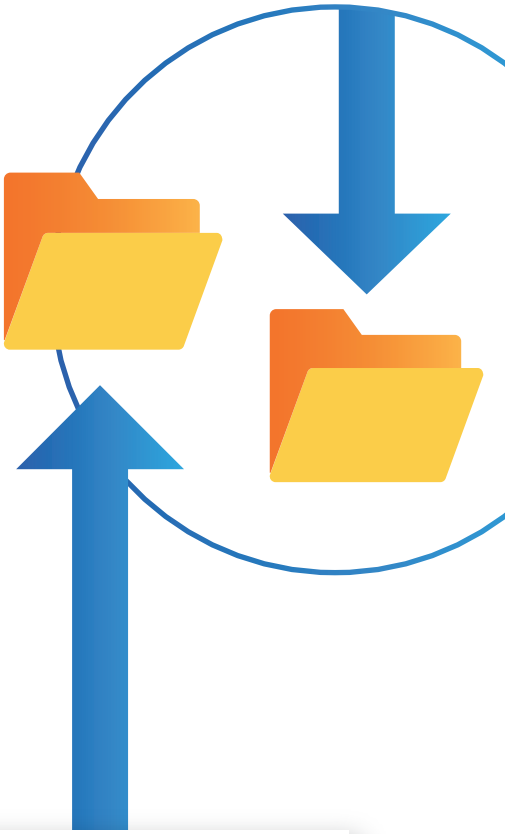
SearchInform SIEM, SearchInform DLP and **SearchInform FileAuditor** are seamlessly integrated: you can connect them to a single data-center, then SIEM will automatically process all the systems' events and add data on them in the console. If required, IS officers can configure, edit and specify rules. For instance, when dealing with access rights to critical resources, IS officer can add resource, which the system should control: for instance, it can be a client database or archive, containing employees' personal data, kept by HR managers. Besides, this rule works regardless of DCAP and DLP: if third parties gain access to a storage, containing personal data, or if a spyware tries to access files – the system notifies an IS officer.

Thanks to the pre-configured rules it's possible to control:

- Copying of large data and file arrays to a flash drive.
- Statistics of access rights changes.
- Employees actions on the specified types of files etc.

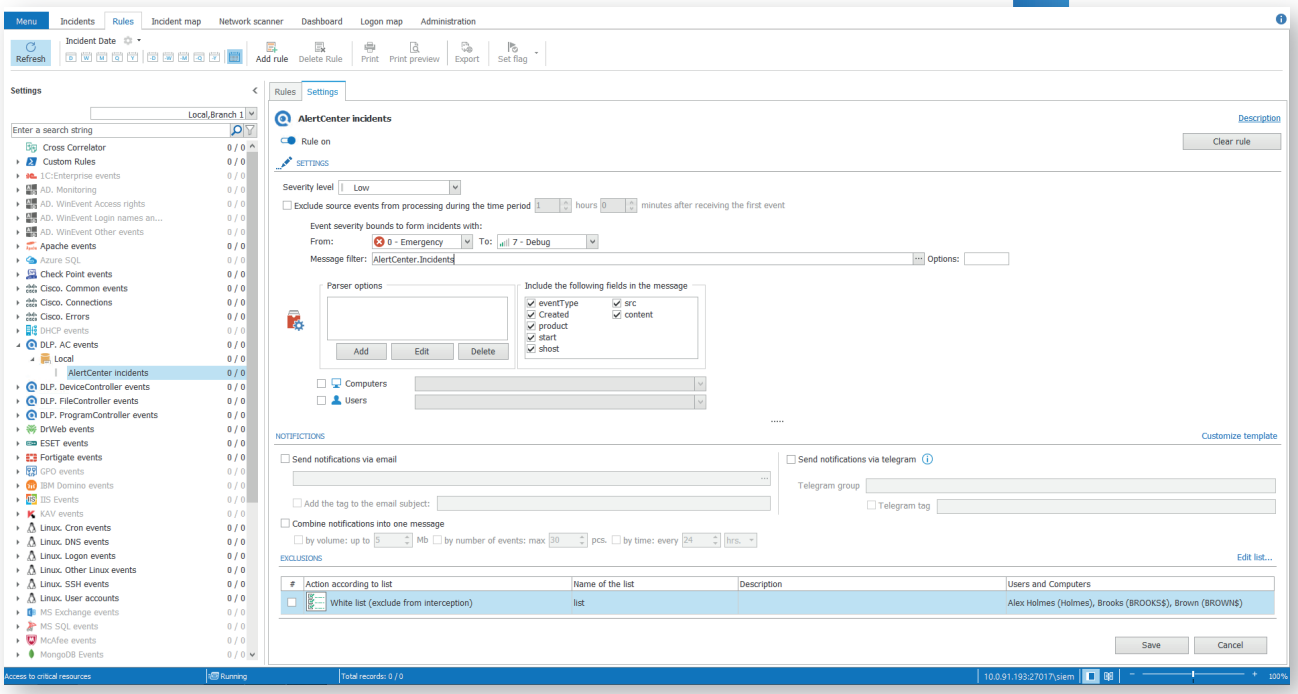
Additionally, you can configure transmission of incidents, revealed by DLP according to the security policies to SIEM.

How to configure?



AlertCenter, DLP's console for management of policies enables to synchronize rules. To do it, it's required to enable data transfer to the SearchInform SIEM and set the timetable for sending details on incidents.

Please pay attention: by default, all incidents from SearchInform DLP will be displayed within one cross-correlation rule; basing on it it'll be required to add new rules. For example, to make the work process more comfortable, rules can be divided into different subsections. In order to add personal data transmission operations to a new category, it's required to add a rule, name it *Passport details transfer* and in the *Message filter* specify the appropriate name of DLP security policy, which transmits data. You can add name manually, it's important to mind the text case. Next, you can turn on notifications on incidents (via email or Telegram), configure exceptions (black and white lists), then the rule will be added to the console.



Configuring AlertCenter incident rules

WHAT IS REQUIRED TO DO IN CASE OF A DATA LEAK INCIDENT?

If personal data somehow leaked, it's required to immediately report the regulator on the data incident and notify clients.

1. Allocate responsibilities between members of a work group

The first thing you need to do is to allocate the employees in charge and divide tasks, aimed at quick incident response between team members.

The work group should include:

- IT and IS departments' employees, as they are in charge of quick detection and blocking of a data leak, assessing its volume, performing an investigation and reporting to the regulator.
- Business department employees, executives and PR department employees notify clients about the data leak. The PR department experts also deal with the negativity in mass media and social networks.
- Lawyers are in charge of assessment and mitigation of legal consequences.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

2. Reporting to the regulator

For example in: **GDPR Art. 33; BDSG p.65**

In many countries there is a requirement to report regulators on data leak incidents. Regulators often require to perform an investigation and reveal incidents' culprits.

Basically, it's required to provide regulators with the following details on the incident:

- event type and category
- incident detection date and time
- details on the data resource
- targeted (in case an external attack took place)
- progress of work on incident response
- assessment of consequences etc.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

In order to conduct a precise investigation:

- Evaluate the volume of data leaked – how many strings leaked, whether critical data was exposed.
- Identify the probable data leak channel: email, copying data to external devices, social networks, cloud services.
- Identify the incident's culprits: find out, whether an internal insider or external malicious actor committed the fraudulent activity. It's also possible, that the data leak incident happened at your counterparty or governmental body side, so check everything precisely.
- Identify the circumstances and find out, whether it was an accidental or deliberate data leak.
- Gather evidence - interview witnesses, download data from DLP, DCAP or SIEM (desktop screenshots, correspondence archive, audit of file system operations, etc.).

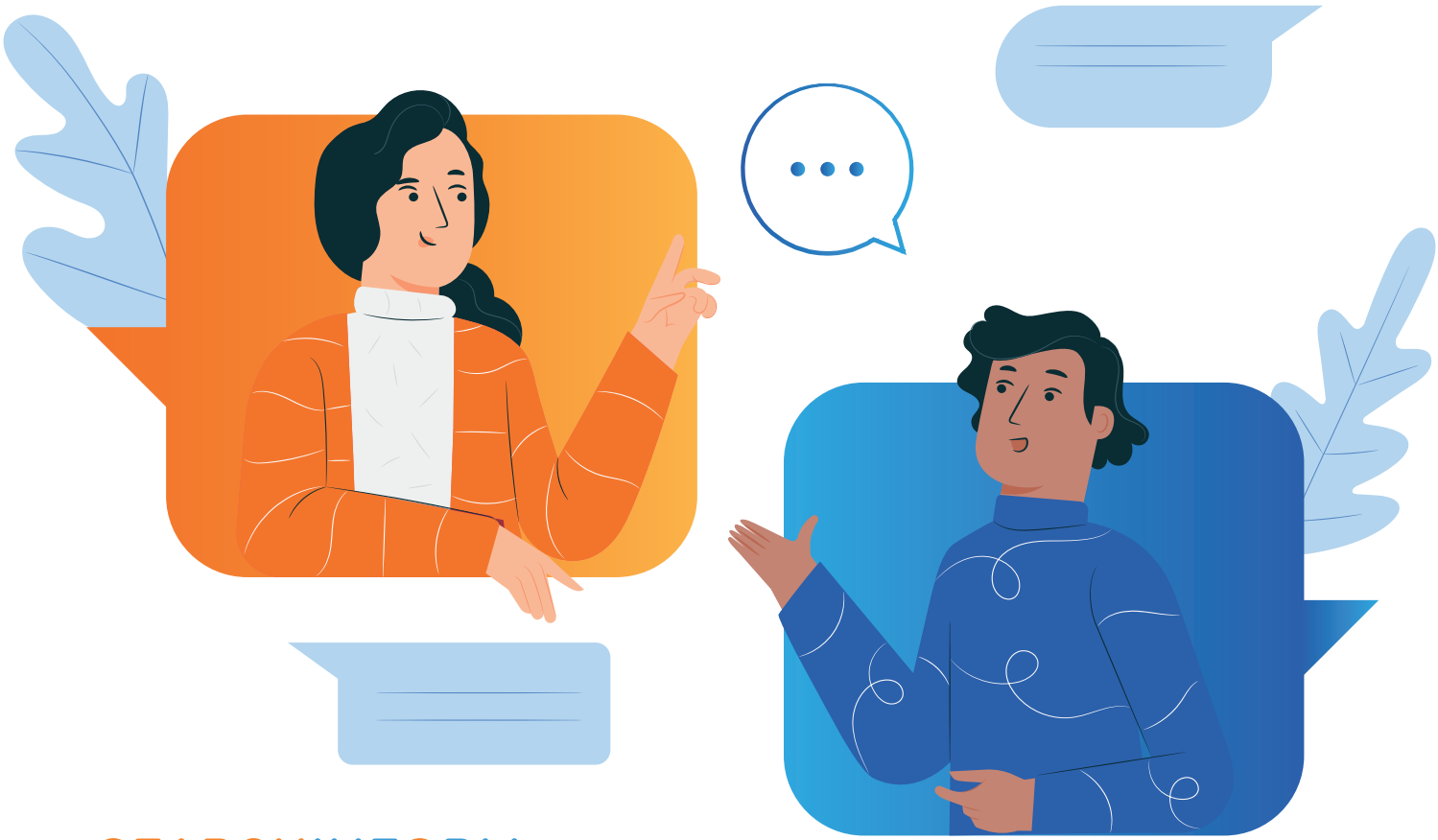
SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

3. Notifying clients

An equally important part for mitigation or the data leak consequences is to explain what happened exactly to all the affected parties. By sending a notification on the data leak, you give them a chance to protect themselves afterwards. For instance, affected parties can change password. Besides, this measure helps you to have more chances to save your reputation: you can explain, what happened before data is published in mass media.

Send a simple and easy for understanding email, containing explanations and your apologizes. Make sure, that the text isn't complicated, avoid usage of professional IS-terms. It's required to explain, what happened exactly, what measures do you take to investigate the data leak incident, what risks does the incident pose to the affected parties and how they can mitigate risks (change passwords, implement two-factor authentication etc.). You can also offer a compensation: bonus, discount or gift.

After apologizing to customers notify mass media representatives about the data leak. It's advised to stick to the following position: "We made a mistake, however, we're working on mitigation of the incident's consequences and we'll do our best not to let such an incident happen again."



WHAT IS REQUIRED TO DO TO PREVENT SUCH INCIDENT OCCURRENCE IN THE FUTURE?

For example in: **BDSG p.64; GDPR art.32; PERSONAL DATA PROTECTION ACT**

First of all, to prevent incidents it's required to ensure advanced information security protection. With the help of DCAP solution you can trace the lifecycle of personal data, in DLP you can trace such data copying, in SIEM – unwanted access to the directories, where personal data is kept. It's helpful to use additional tools in IS solutions, such as user notifications and blockings, as they help to mitigate risks significantly.

Secondly, it's crucial to follow other preventive measures as well:

- Enhance employees' IS literacy. Explain, what is phishing and what techniques do fraudsters implement to perform phishing attacks; reveal, what risks do emails, sent by unknown users pose; tell, how accidental download of malware can lead to the theft of confidential data; remind about the importance of complicated passwords and necessity to log out when leaving workplace.

- Introduce liability for disclosure of confidential information and data leakage. Sign an NDA (non-disclosure agreement) with employees. Employees must understand the responsibility for disclosing critical information.

- Put everything in order in the corporate IT-infrastructure: limit access to important documents, figure out which network folders they should be in, set up two-factor authentication for access to critical services, use encrypted data channels, etc.

Prevention will reduce the risk of the incident happening again. This is not a one-time action; such measures should be permanent.

Request consultation with our experts on how to comply with the regulators' requirements.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

SearchInform is one of the leading risk management product developers. For over a decade the company has been a technological trailblazer focusing on contemporary cybersecurity threats, protecting business and government institutions against data theft, harmful human behavior, compliance breaches and incomplete audit.
More than 4000 companies across all major economic domains, from banking and retail to machinery and fighter jet manufacturers, count on SearchInform regarding efficient holistic risk management solution defending against ever-improving threats and allowing you to avoid ominous consequences.

SearchInform **DLP** helps you know your data and put controls just right where you need them to protect the company from confidential information leakage. SearchInform DLP monitors all popular data transfer channels, analyzes information, detects and prevents violations, provides reports to the person in charge.

SearchInform **FileAuditor** is a DCAP solution (data-centric audit and protection) intended to help the companies to identify sensitive information in the file system, audit information storages, detect access violations and track changes made to critical data. The system protects confidential documents from careless and deliberate malicious actions of employees and puts things in order in file storages.

SearchInform **SIEM** is a system for collecting and analyzing real-time security events, identifying information security incidents and responding to them. The system accumulates information from various sources, analyzes it, records incidents and alerts the designated staff.

SearchInform **Risk Monitor** platform conducts real-time analysis, identifying every ongoing event within the network. SearchInform Risk Monitor aids your company in building a risk management program and a solid insider threat management process, helping to foresee potential internal corporate risks in advance and offering forensics tools.

Service model and deployment in the cloud

Ensure data protection and fulfill regulatory requirements without hardware purchasing and labor costs.

Find more useful materials on the information security related issues on SearchInform website