KP CERC

CYBER EMERGENCY & RESPONSE CENTER

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR

General Data Protection Regulation

DR. Rafi us Shan,

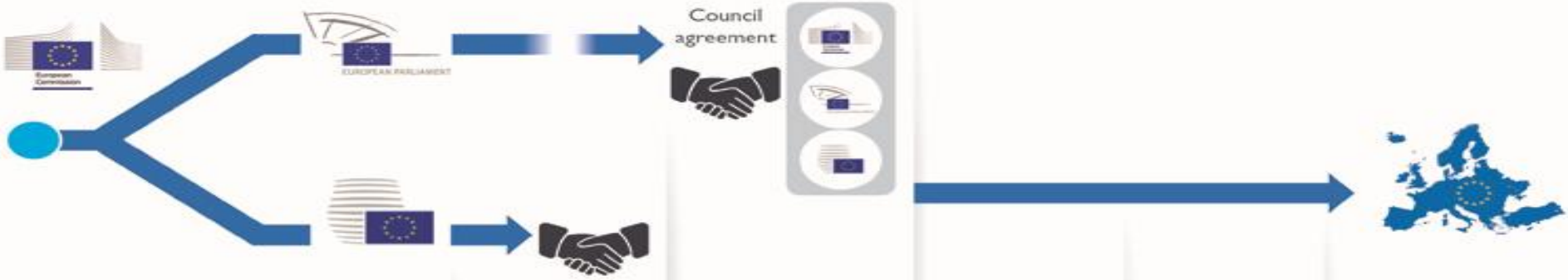
Chief Cyber Security , KP CERC

KPITB

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa
KPITB

GDPR TIMELINE



European Commission publishes the legislative proposal	Separate negotiations within Council and European parliament	EP reaches agreement	Negotiations and approval among the three institutions	Regulation published in the Official Journal	Two years implementation phase	Regulation applies from
2012		SPRING 2014	2015	27 APRIL 2016	2016 2017	25 MAY 2018

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Definitions

- GDPR is a set of EU laws that come into affect on May 25th 2018.
- GDPR rules are designed to give more control over personal data.
- GDPR is a European Commission regulation/law for the protection of data and privacy for all the European Union (EU) and the European Economic Area (EEA).

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Regulation

REGULATION

- (EU) 2016/679 (88 PAGES)

DIRECTIVES

- (EU) 2016/680(43 PAGES)
- (EU) 2016/681 (18 PAGES)

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Everyone follows the same law

- Regulation will ensure that everyone abides by the same rules. Everyone should follow the same law.

One-stop solution

- Hugely beneficial for businesses as they will have to deal with only one regulatory body, making it simpler and cheaper for companies to do business in the EU.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR Objectives

- Main objective is to protect the privacy of citizens of the EU and unify the data regulation rules of the EU's member nations.
- Purpose is to provide a set of standardized data protection laws across all the member countries.
- Regulates and addresses the flow of personal data outside the EU and EEA areas.

Explanation

- GDPR also applies to foreign countries using the data of EU countries.
- Regulation has been made stricter than originally planned and 4% of the turnover is penalized in case of non-compliance.
- There are numbers of challenges upon the implementation of GDPR.
- Biggest challenge will be for businesses to update their practices according to the regulations.

GDPR PRINCIPLES

1 Lawfulness, Fairness and Transparency

Lawful: Processing must meet the tests described in GDPR.
Fairness: What is processed must match up with how it has been described.
Transparency: Tell the subject what data processing will be done.

2 Purpose limitation

Personal data can only be obtained for "specified, explicit and legitimate purposes". Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

3 Data minimization

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". i.e. No more than the minimum amount of data should be kept for specific processing.

4 Accuracy

Data must be "accurate and where necessary kept up to date".
Base lining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

5 Storage limitation

Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary". Data no longer required should be removed.

6 Integrity and confidentiality (security)

Requires processors to handle data "in a manner (ensuring) appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage.

7 Accountability

The controller shall be responsible and be able to demonstrate compliance.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Right To Access

Data subjects have the right to obtain confirmation from data controller of their personal data are being processed and should provide an electronic copy of data for free to data subject.

Breach Notification

Event of data breach, data processors have to notify their controllers and customers of any risk with in 72 hours.

Consent

Obtaining consent for data use, companies can not use indecipherable terms andconditions. It must be as easy to withdraw consent as to give it.

Privacy By Design

Calls for inclusion of data protection from the onset of designing systems, implementing appropriate technical and infrastructural measures.

Data Protection Officers

Professionally qualified officers must be hired in public authorities.

Specific Permission

Give permission to an app or website to use your details, they can't use it for any other purpose or sell it to third parties.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa
KPITB

Information In Clear Readable Language

Right of the individuals to get the information and put new rules at an end as privacy policies and that information should be given in clear and plain language before any data is collected.

Limits On The Use Of Profiling

Under GDPR, profiling will be allowed with the consent of the person concerned, where permitted by law or when needed to pursue a contract and requires human intervention.

Right To Be Forgotten

Under the GDPR you have a right to be forgotten and will be able to ask companies or platforms to delete your data.

Data Portability

Get the right to ask for any data that a company has about you in a readable format so that you can reuse it.

Adopting Techniques

The new rules promote techniques such as:

- Anonymization (removing personally identifiable information where it is not needed)
- Pseudonymization (replacing personal identifiable material with artificial identifiers)
- Encryption (encoding messages so only those authorized can read it to protect personal data)

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR Compliances

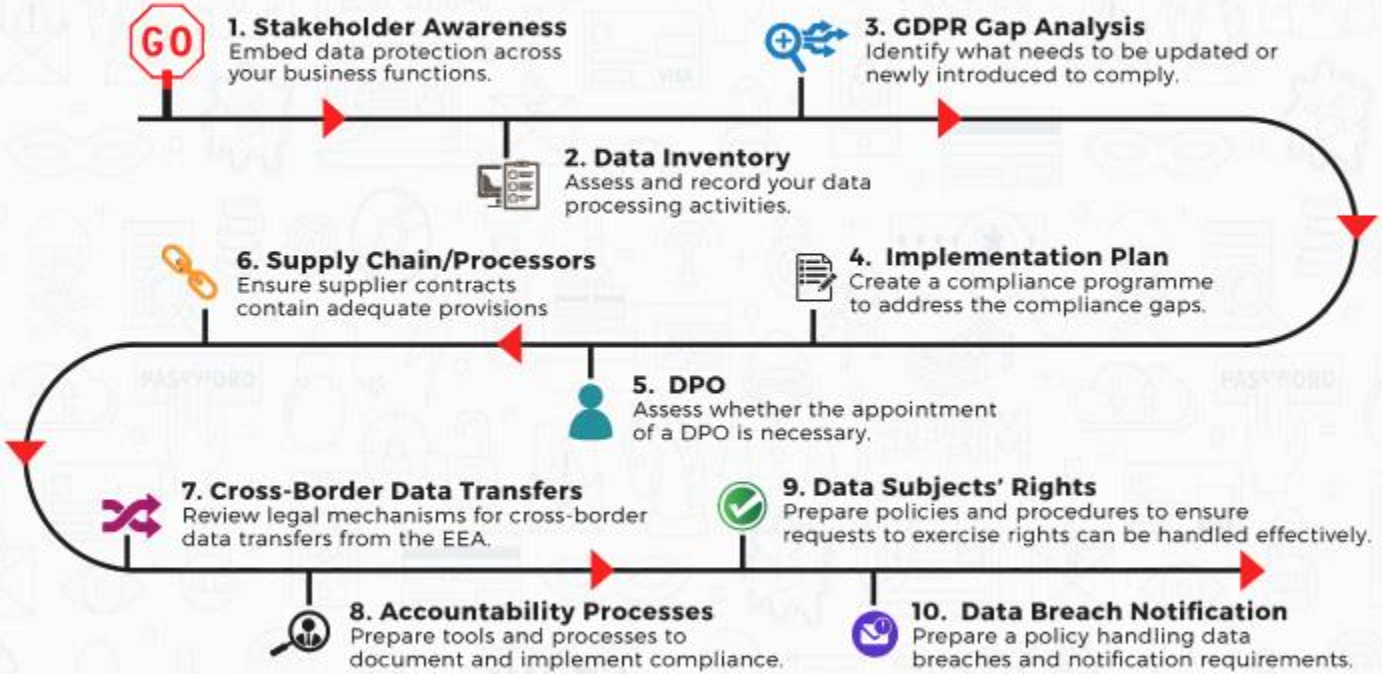
- Data breaches inevitably happen.
- Information gets lost, stolen or otherwise released into the hands of people who were never intended to see it.
- Organizations will have to ensure that personal data is gathered legally and under strict conditions.
- Who collect and manage it will be obliged to protect it from misuse and exploitation.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR: THE PATH TO COMPLIANCE

HELP YOUR ORGANISATION STAY COMPLIANT WITH THIS 10 STEP GUIDE



Info source: *reedsmith.com*

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR Data Handlers

There are two different types of data-handlers.

The legislation applies to “Processors” and “Controllers”

- **Controllers**
- **Processors**

GDPR Data Handlers

Controllers

- Owners of the data.
- Responsible for data security.
- Controllers are not relieved of obligations.
- Controllers determines the purposes of processing personal data.
- GDPR places further obligations on controller to ensure their contracts with processors comply with the GDPR.

Processors

- Work with data.
- Involve in relieved of obligations.
- Must take responsible actions with data.
- Responsible for processing personal data.
- Processors has legal liability and are responsible for a breach.
- Required to maintain records of personal data and processing activities.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Compliance Components

- These are 3 Basic Compliance Components which are good for Company.
- These 3 components will be apply on collected data.

1. Comprehensive Data Protection
2. Proof of Data Security
3. Data Breach Control and Response Planning

1: Comprehensive Data Protection:

- Consumer’s personal data must be protected at every stage of its lifecycle with a company.
- Protecting data at rest includes tracking, monitoring and limiting access (both remote and physical) to network resources and data.
- Companies must also properly vet their business partners and all parties with whom they share data, to ensure they abide by data protection regulation requirements as well.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

Organizations must employ network protection measures including

- Firewall configurations.
- Current, updated antivirus software.
- Data tracking, monitoring and reporting.
- Limited access to servers and networks.
- Sophisticated credentials creation and verification measures.

Benefits

- Data security efforts do more than just protect the customer and the business from breaches and leaks.
- Force organizations to fully understand their complicated data webs in order to effectively secure them.
- This can slow down the rampant land grab for all things data, as organizations realize they can’t merely own data.
- Organizations have to understand it, use it, and conscientiously protect it.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
KPITB
Government of Khyber Pakhtunkhwa

2: Proof of Data Security:

- Burden of proof is on organizations that claim to be compliant with data protection regulations.
- Provide evidence that they are indeed monitoring and protecting their consumer data.
- Requires the use of action logs and audit logs, which can track data transactions and demonstrate which data controls are in place.

- Regular analysis and verification is also necessary when it comes to proving data security and compliance.
- Companies can perform security audits, vulnerability assessments, and penetration testing, among other efforts, to ensure all requirements are in place and are working properly.
- Employ data management tools that facilitate compliance through settings and automation and are designed to generate reports to help audit compliance status.

Benefits

- Provide proof of data protection prompts organizations to self-assess their data security and self-enforce requirements and standards.
- Corporate accountability, which only stands to benefit a company.

3: Data Breach Response Planning

- Company have a response plan for breaches or leaks, including a notification plan to inform whose data has been compromised.
- Establish, document, and share a Breach Response Plan with key stakeholders.
- Ensure third-party partners and service providers understand breach policies and implement breach response plans of their own.
- Identify a "Breach Response Team“, including representatives from IT, Communications/ PR, HR, C-level, and Legal.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa
KPITB

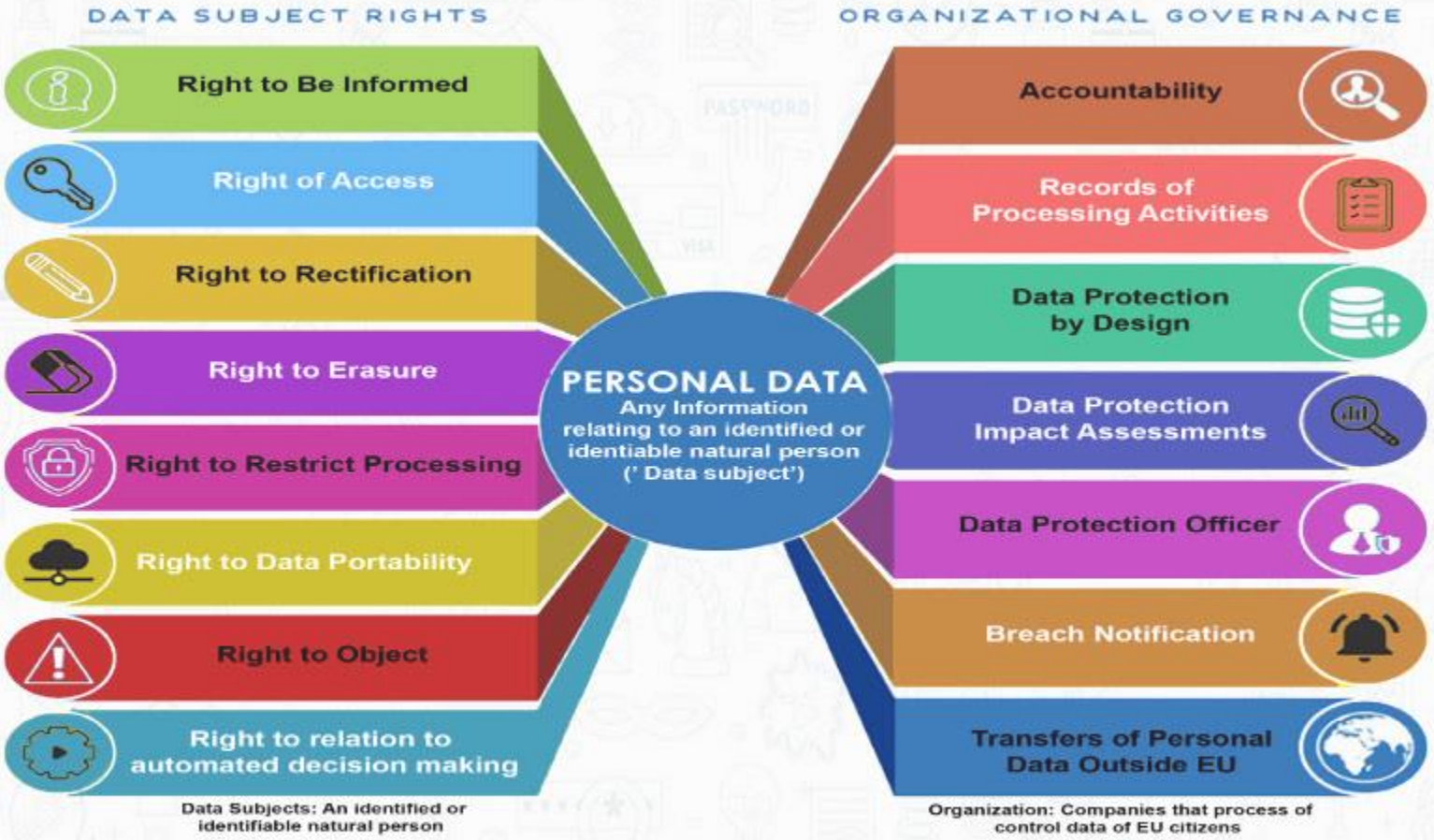
- After a breach is contained, perform a vulnerability assessment to identify weak spots and determine the point of failure.
- Create and execute a breach mitigation plan as well as any preventative steps to avoid a reoccurrence of the incident.
- Notify external parties who are affected by the breach, and provide a description of the breach, a key point of contact, and measures taken to mitigate the situation.
- Document all actions regarding the breach, from discovery through notification and beyond.

Benefits

- Having a solid breach response plan, companies essentially subscribe to the principle of expecting the best, but planning for the worst.
- It’s crucial to be prepared for high-stress, potentially costly situations such as a leak or a data breach.
- Data protection regulations might require this level of preparedness.
- Organizations should have any way for regardless of compliance.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa



KP CERC
CYBER EMERGENCY & RESPONSE CENTER

Info source: *www.mentisoftware.com/GDPR*

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR Fines and Penalties for Non-Compliance

Failure to comply with GDPR can result in a fine ranging from 10 million euros to 4% of the company's annual global turnover, a figure which for some could mean billions.

The maximum fine of 20 million euros or 4% of worldwide turnover. Unauthorized international transfer of personal data, and failure to put procedures in place or ignoring subject access requests for the data.

A lower fine of 10 million euros or 2% of worldwide turnover will be applied to companies which mishandle data in other ways.

Fines will depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner.

Failure to report a data breach, failure to build in privacy by design and ensure data protection is applied in the first stage of a project and be compliant by appointing a data protection officers.

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

GDPR Advantages

1. Improved Consumer Confidence
2. Better Data Security
3. Reduced Maintenance Costs
4. Better Alignment with Evolving Technology
5. Greater Decision-Making

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

What to Do NOW?

- Make key departments aware
- Workout what you have
- Get your minimum technical steps in progress
- Revise existing privacy notices
- Review procedure for new rights
- Plan how to handle requests
- Document your legal basis for your use of data
- Review how you get consent and record it
- Procedures for data breaches and checks
- Appoint a data protection officer

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KPITB
KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

Thank You

KP CERC
CYBER EMERGENCY & RESPONSE CENTER

KHYBER PAKHTUNKHWA
INFORMATION TECHNOLOGY BOARD
Government of Khyber Pakhtunkhwa