ELTE - Faculty of Informatics

Subject: Privacy Lecture

Lecturer: Dr. Péter Ligeti

Privacy issues of the data management related to COVID-19 in Germany and Pakistan

Date of submission: 15th of June 2022

Ali Aqeel Zafar (AAFZDE)

Friedrich Ostertag (D7KQBF)

Content

1. Introduction

In this essay, we will introduce the privacy situation and data regulation policies in Germany and Pakistan. First, we will go through both countries and explain, which regulations were in place, problems that occurred during the COVID-19 pandemic from a privacy point of view, and if there were any changes to the policies. Following this, we compare both countries in various aspects, as the structure and legal rules about data handling during the pandemic. Finally, we analyze the German covid-warning-app to find out if it ensures privacy and if there are possible attacks.

2. Privacy situation in Germany during COVID-19

Let us start by taking a look at Germany's data management in the COVID-19 pandemic and issues arising from that. I will begin with an introduction of the legal background and basis in Germany.

2.1. Legal background in Germany

Since 2018, the GDPR (General data protection regulation) applies in Germany. This regulation is specified in Germany through the BDSG (Bundesdatenschutzgesetz) which implements the GDPR on a national basis. In case of conflicts, the BDSG is subordinated to the EU-wide GDPR. Furthermore, in Germany each of the 16 federal states has some freedom when it comes to interpreting those privacy laws. Aspects that fall within this room for interpretation include for example who exactly is responsible for the data privacy and protection within a company / authority and what appropriate means for storing and processing data are. Inspecting each of those individual federal instances of the BDSG might be interesting for handling a lawsuit, but would be too detailed for this essay. That is why I will not deal with their specifications and instead continue with a focus on the general BDSG guidelines under which all the federal rules fall. The BDSG requires (same as the GDPR) data minimization to the purpose, privacy, transparency about the data processing, data security and adequate data deletion. That is after one month for covid-tracking related data. I am highlighting those aspects here, as I consider them to be most relevant ones in the context of data handling in the covid pandemic.

2.2. Involved public authorities

In Germany, there are three pubic parties involved in handling the covid-crisis. The separation of the tasks in between these three allows for data minimization, as each authority only gets the data required to fulfil its tasks.

First, there is the **Paul-Ehrlich-Institut,** which is responsible for vaccination and medicament safety in general. Its job in the pandemic is to test and approve vaccines, monitor the use of vaccines and their safety and give recommendations regarding vaccinations. Doing so requires huge amounts of data.

Then there is the **Robert-Koch-Institut (RKI)**, which is the national public health institute in Germany. This institute is responsible for fighting infectious diseases. That means monitoring of how many people are infected, how severe the infections process and where and how infections are spreading.

The last big party involved are the **national and federal public health agencies.** Their job is to ensure the compliance with covid related restrictions. That means checking, if companies implement covid rules correctly. Also, the behavior of private individuals must be tracked by these authorities. Enforcing quarantines and tracking contacts falls under their responsibilities. This requires the most sensitive kind of information, as contact and quarantine tracking is not possible without precise personal information.

Data processing by public authorities

While the health agencies do not publish any data and only contact persons affected by rules, the Paul-Ehrlich-Institut and the RKI do publish results from their analysis. Since that published data contains only general information, as anonymous vaccination and infection numbers, and no personal information, there are no privacy concerns regarding the publications. However it is not public how the data is processed within these authorities, and if that is done according to the BDSG. I claim this can be assumed, as data protection officers are in charge in each authority and no data leak has been revealed yet.

2.3. Covid related data processing implications of the GDPR

For tracking contacts and fighting the pandemic there were rules in place that required the collection of personal information especially for companies offering physical services. Companies like restaurants, bars, hairdressers, beauty salons, massage and tattoo studios. For a certain period, only people with a valid immunity certificate were allowed to enter those. Furthermore, there was a reporting policy for companies in case there were covid positive cases within their employees. I want to clarify next, how those tracking mechanisms were implemented and what measures were allowed and not allowed according to the BDSG to comply with the regulations. I will begin with how the contact tracking was implemented in Germany, followed by quarantine rules, travelling and the immunity certificates.

Contact tracking

For physical service companies it was obligatory to keep contact information of the customers. That was done by two different methods. Either a paper-based list was provided, on which the customers had to write down their name, address and contact information. The other way was to use a mobile tracking app, the Luca-App which is privately run by a profit oriented company. The app could be used to scan QR-codes provided by the service companies to check-in.

For the Luca-App, one must register with personal data as name, address and phone number to the app. The app stores the location data encrypted on a central server for 30 days. In case of a positive covid test, a user or a company could alert the app and each user who was at the same location during the same time would be informed. Additionally, data about covid positive persons and data about his/her contact persons of the last 14 days could be shared with the public health authorities. In general, the tracking data must be deleted after 4 weeks. The hosts / companies are responsible for collecting and deleting the data, while the guests / customers are responsible for the correctness of their provided information.

Quarantine rules

Now I want to continue with how the quarantine rules were applied. Enforcing quarantines is the task of health authorities. They can do that by calling/visiting people in quarantine to check if they are actually home. In extreme cases, personal data may be shared with the police. But only if that is needed for quarantine enforcement. Otherwise, no personal data about covid positive persons should be shared with any third party.

Leaving/entering country

Upon leaving/entering the countries there were also some rules for a time-period, which were especially applied at airports. That contained checking the paper based or electronic immunity certificate but no data storing. If a person had to do quarantine, his or her data was transmitted to the health authorities upon entering the country. But even then it was not locally stored at the point of entering Germany.

Vaccination data

The last point on this list is about the digital immunity certificates and their required data. Upon a positive PCR-test after infection or a vaccination, the data was sent to the RKI, where it was validated and signed. Data means name, date of birth, country of vaccination, certificate provider and an id number of the certificate. The RKI only stored the data temporarily for this purpose. With the verified and signed certificate, one could prove immunity while only revealing name, date of birth and the immunity status. The name and date of birth could then be compared to the passport/id of that person.

Legal actions

Legal measure for companies include voluntary questionnaires and voluntary temperature checks for the employees. Asking about direct contact with covid positive persons and recent stays in risk areas was allowed and the employees were obliged to answer those questions truthfully. Upon request, data about covid positives, contact persons of covid positives and information about people staying in risk areas had to be transmitted and shared with the public health authorities. Contact information about the employees to send warnings/information about rules at the workplace was only allowed to be collected with the agreement of the employee. If contacts were tracked in paper-based form, the list had to be stored in a secure place and be maintained in such a way, that no customer was able to see the entries and data of other customers.

Illegal actions

In contrast to that, generally asking all employees about their current state of health or their travel plans was not legal. Implying rules to report colleagues showing illness symptoms was also not allowed, as well as publishing who was covid positive or any personal information about covid

positive employees. No data concerning covid related activities was allowed to be processed in any way besides sharing with the authorities.

2.4. Changes in the publication policies during the pandemic

In Germany, no changes have been made to the existing data processing policies. Changes only affected who and what data should be collected at what time. The rules regarding the processing of that data remained the same as before the pandemic. So let us look at the changes and their implications on privacy.

With a change in the Bevölkerungsschutzgesetz (law for citizen safety) hospitals and doctors became obliged to send data related to certain germs (in this context especially covid-viruses) to the RKI so that it was better able to continuously assess the situation and be aware of changing circumstances. Besides that, personal data related to vaccinations should be sent to the Paul-Ehrlich-Institut by those medical parties to track the vaccination progress and the vaccine safety and possible (side) effects of the different vaccines.

Those changes were covered by the existing BDSG rules, as the means were considered as adequate to allow the data transmission. Of course, the receiving and sending parties had and still have to comply with the privacy rules regarding the storing and further processing of that data.

2.5. Further issues

In this chapter I would like to discuss some more issues in the context of covid related data processing.

Conflict of fighting the pandemic vs. keeping privacy regulations

Because of the pandemic, more sensitive information than ever was stored. On the one hand fighting the pandemic becomes more efficient the more data there is available. On the other hand, companies and authorities were not prepared for those amounts of data. Regulations were not complied with, data controllers were not always in place or not involved, data was stored insecurely and/or not deleted in time. That led to an increase of malicious activities and many leaks of sensitive information.

Constantly changing policies

Constant changes in the rules and policies required companies and employers to always stay informed and apply those changes to their data collecting/processing mechanisms. That was especially for small companies not easily feasible so that often companies were lacking behind the current rules and regulations and did not delete data in time.

Problems with physical contact tracking

The next problem emerges from the physical, paper based contact tracking. To make things easier many companies used one big list, where everyone would just type in his/her contact information. According to the laws that was illegal. There should have been one piece of paper for each person to prevent each of the customers seeing sensitive information about each other. Also, a data processing declaration would have had to be handed out when collecting the paper-based information. That would have led to lots of paper work, and would have been very time consuming for companies as data collectors and customers as data subjects. Acting according to the law was very impractical due to these reasons and not often correctly applied.

Problem with control

The last problem is the control of company's data processing by the federal data protection office. As there was and is not enough capacity to control every party collecting data throughout the pandemic, only random samples are controlled. De facto there was no official control, whether companies complied with the data regulation laws regarding data processing and deletion of the sensitive personal information collected.

3. Privacy situation in Pakistan during COVID-19

Pakistan is a developing country and has many political tensions going on during COVID-19. Along with tackling the pandemic, the country has many privacy issues in regards to data management during the pandemic. The most important one is that there are no general regulations or laws in terms of data protection and data management made by the federal government that can be followed by every organization in different economic sectors. Because of that during the pandemic, several patients' valuable information was leaked by adversaries.

Hospitals do not have any secure data protection and management policies. In addition, a major factor is politics because the governments of different provinces want to establish their own data protection and management laws even if the federal government does not allow it. On the other hand, the federal government wants to have common laws and regulations, but the government of different provinces does not agree with it. During these past two years of the pandemic, several laws and petitions were drafted in National Assembly and Provincial assembly for having a standard privacy protection law and regulation but none was passed in the end.

Another reason is, that the experts that are part of the Executive Committee of Information Technology do not have that much experience and have catered to privacy issues in data management as well. For example, when the first COVID- 19 wave was undergoing, the executive committee developed a contact tracing application, which also included the volunteers' contact information, so that patients could take guidance from them as well. Due to a lack of data protection and data management policies, the information of the COVID-19 patients and the volunteers circulated on different social media platforms, as well as sold to some unofficial personnel.

3.1. Legal Background

At the moment, Pakistan does not have any specific law related to data protection and management. However, in January 2021, the Ministry of Information Technology and Telecommunication drafted Pakistan Personal Data Protection Bill, 2021. The bill is still under consideration to date in Parliament. This bill will apply to all the sectors, which are existing in the country. If the bill is approved by the Parliament, a governing body will be made that will be responsible that all the organizations conform with the general law of data protection and management. The governing body's name will be the Personal Data Protection Authority of Pakistan. General privacy regulations for private companies were not in place, but voluntary standards existed in different industries (e.g. Banking, IT, etc). This led to multiple privacy issues in different industries, but none of them is especially relevant in the context of the COVID crisis, as all the COVID related data was handled by the government and not private companies.

3.2. Publication Policy

The publication policy that is being used by Pakistan is the Pakistan Dissemination Policy. This policy is followed by every sector currently present in Pakistan. The governing body is FBS. The data is collected from primary and secondary sources. The primary sources are through different surveys like Labor Force Survey etc., while the secondary source is from the statistics like

Industrial Statistics, Foreign Trade Statistics. According to the previous policy, the data was supplied for free but now it is not according to the current policy. FBS has revised the overall policy according to some things as follows:

- The format in which the data should be supplied to maintain the confidentiality of statistical data, the micro-level should be supplied in tapes or disk after removing the micro-level identification only after publication of the report.
- The user shall provide an undertaking that data collected from FBS will not be supplied to any other person or organization. The user shall acknowledge the source of data and supply copies of the research work or articles to FBS.
- It should be ensured that the statistics supplied will not in any way the identity and state of affairs of any individual, firm, or institution according to General Statistics Act,1975.
- Only the intended data should be given to the organization and the organization for their specific purpose which they informed FBS before collecting the data.

This policy applies only to data that is shared by the government with other parties and regulates, how those other parties should process and handle the data.

3.3. Covid Data Management

In this chapter, I will explain, how COVID-19 related data was managed in Pakistan. I will go through how data was collected, processed, stored and tracked.

3.3.1. Data Collection

People who got covid if they tested positive their results were sent by hospital or laboratory automatically to the National Institute of Public Health. This institute then sent a text message to the infection person stating that their data regarding being Covid positive was stored in Institute's custody. Similarly, for people, while entering or departing from or to the country, the Covid test is done also, and if it is positive, it is then sent to the National Institute of Public Health and it is stored in their databases. In addition, the institute according to the Pakistan Dissemination Policy can ask for the data of citizen from FBS (managing authority) and saves it in their databases. In case the patient dies due to Covid, the institute updates its data as soon as the hospital informs the demise of the patient. The data collection process is done on daily basis by the institute.

Data regarding vaccination was collected and administered by the National Institute of Public Health. People registered on the official website, and their data was collected by the institute. The

National Identity Card number was used as the primary identifier to manage vaccination history by the institute.

3.3.2. Data Processing

After collecting data National Institute of Public Health sends the data to the Ministry of Information Technology so that the analysis and processing of the data. This is done in order to make a statistical analysis like which province is highly infected, which areas are highly infected, how many deaths occurred, what is current covid positivity, and how many are vaccinated now. Ministry of Information Technology is responsible to do the statistical analysis and processing and also updates and looks after the contact tracking application. There is no exact information about how the ministry processes the data as they do not publicly disclose this information, but sources like doctors who are part Covid 19 team say, that they have their own proprietary software which is responsible for processing the data. After the processing of the data and doing statistical analysis, the Ministry of Information Technology informs the National Institute of Public Health regarding the data processing results. The Public Health Institues then decides about measures like smart lockdown or stricter covid rules and regulations in the country. The data is being transferred between both the government organizations and the consent is taken by the patients from before when they sign a consent form before taking the covid test or registering themselves for vaccination. Those processing mechanisms are stated in the consent form.

3.3.3. Data Storage

Due to security issues, both organizations did not publicly disclose on their websites how the data of Covid 19 is stored. Only a handful of people working in these organizations mentioned that the data is stored separately in the databases of these organizations and also in the disaster recovery site, where a copy of the data is kept.

3.3.4. Data Tracking

People while entering or departing from the airport, bus stations, and train stations their Covid test reports and vaccination reports are checked, meaning the bar codes on their respective reports were scanned. The bar code is linked with the National Institute of Public Health database along with the database of the Ministry of Information Technology. Also, for people going to public places, their Covid vaccination and their Covid vaccination report barcode were scanned so that if anyone broke the rules, serious action could be taken against them. After scanning, the bar code redirected to the National Institute of Public Health's website. The page contains information like name, national identity card number, Covid test results, from where the person took the Covid

test, which pharmaceutical company's vaccination they took, which it is, and the location from where the person took the vaccination from. People's consent was taken before taking the Covid test or registering for the vaccination stating that during traveling or going public places officials are allowed to scan the bar codes of vaccination certificates and the Covid test certificates in order to check the authenticity of the certificates.

3.4. Contact Tracking Application

The Ministry of IT and Telecom and the National Information Technology Board developed the contact tracking application. The application provides dashboards for each province and state, self-assessment tools, and hygiene reminders. It also statistical analysis regarding how many people are vaccinated, percentage of people which taken first, second or boosters doses. The initial version of the application should location of the Covid positive as their home addresses but now it has been removed by the Ministry of Information Technology, as it was leaking location data, thus endangering privacy. The application also showed Covid saturation in a particular part of city or province. It showed the Covid positivity rate as well in the whole country, province and city as well.

4. Comparison of the situation in Germany and Pakistan

In this chapter we will compare both of the previously introduced countries in regards to the governmental authority structure, data processing in the private industry and the contact tracking and quarantine enforcement.

4.1. Comparison of the legal environment

Pakistan's regulations focus on the publication of data and only include data that is shared by the government with private companies. For processing, sharing and publishing data that was collected by or from companies and not the government there were no specific laws in place. That did not result in any additional problems during the pandemic, as COVID related data has been exclusively processed by the Pakistani government.

In comparison to that, German companies were also involved in processing specific data to fight the pandemic. That opened the door for lots of data misuse potential and required regulation. The publication of personal information is in almost all cases prohibited in Germany, according to the BDSG. The BDSG also covers the processing of data, meaning which information should be

collected for the mean of fighting the pandemic, how should it be stored and for how long. Those regulations through the BDSG apply to private companies, as well as the German government.

4.2. Comparison of governmental authority structure

In Pakistan there is the Ministry of Public Health and the Ministry of Information Technology. Those two form a central entity where all data is stored and processed. The Ministry of Public Health manages how and which data is processed, while the Ministry of Information Technology does the processing according to request from the Health Ministry. In words of the GDPR, the Ministry of Public Health is the data controller, while the Ministry of Information Technology is the data processor. Information collected include name, age, address, ID number, vaccination details, COVID test details.

In contrast to that, the tasks are more split up between German authorities. There is the RKI which is responsible for managing and monitoring the pandemic, the Paul-Ehrlich-Institut, which has to track and ensure vaccine safety, and the public health agencies, who's job it is to enforce quarantine rules. That allows for data minimization, as each authorities only receives the data required to fulfil its specific task. For example the Paul-Ehrlich-Institut only gets data related to vaccinations, while the sensitive personal information required for contact tracking are only processed by the public health authorities.

4.3. Comparison of data processing in the private industry

The only additional data processed by Pakistani companies within the pandemic were the QR codes to verify immunity and/or COVID test results. There was no data storing at private companies, they only got an insight to the relevant information of the public health entry of the scanned person.

Similar to that, in Germany certain companies also had to verify the immunity status and/or test result of customers. That was possible by showing either the paper based certificates, or a scannable QR code which allowed verification.

Unlike in Pakistan, German companies offering physical services were obliged to collect and store contact information from their customers for 30 days. They were not allowed to use, share or process that data in any means besides transmitting it to the public health authorities upon request.

4.4. Comparison of health status verification

In both countries the COVID rules required citizens to show test results and/or their immunity certificate when entering certain locations. That was implemented similarly with QR code technology and in both cases the verifying party got access to minimized data required for verification of the test result / immunity certificate. The access was only temporary for the time of entering and no data had to be further stored / processed. In Germany it was also possible to provide the paper-based documents for verification. Those could reveal more information (if not covered), but the risk of misuse was still negligible (someone would have to remember the information from looking at the paper and then write them down for storing).

4.5. Comparison of contact tracking and quarantine enforcement

While there were quarantine rules in place in Pakistan, there was no strict enforcement. It was not checked, if COVID positive people quarantined, or with whom they were in contact with. While that might not be the most effective way of fighting the pandemic, no privacy concerns occur either.

In Germany, the health authorities were randomly calling or visiting quarantined people to check if the quarantine rules were complied with. Also, COVID positive people were questioned about the locations they recently visited and then those locations would had to share their guest-tracking lists with the health authorities. That allowed for effective contact tracking and quarantine enforcement in theory, while in reality the authorities were only able to handle a small percentage of the cases due to understaffing. Unlike in Pakistan, the German health authorities handled lots of sensitive personal information and location data for those means. That had to be done in compliance with the BDSG.

4.6. Conclusion

To summarize this chapter we can say, that the gap between Pakistan as a developing and Germany as a developed country is also visible when it comes to data regulations and fighting the COVID-19 pandemic. The data regulations in Pakistan only apply to a very limited set of data, while the GDPR and BDSG are very comprehensive approaches to regulate data processing. Still, in both countries no rules were changed and no new regulations were implemented in the context of the pandemic. The immunity verification was done very similarly as well.

As there were less covid related rules in Pakistan, less data had to be collected and processed thus the need for a complete data regulation law was not as high as in Germany. Nevertheless, it

would be an important step to implement such laws, not only in case of pandemics. That could improve citizen safety, transparency and democracy. The future will show, if and how Pakistan will adapt to the digital world and issue data policies.

5. COVID-19 tracking application analysis

In the final chapter of this report, we want to introduce the German COVID-19 tracking app (Corona-Warn-App), and analyze it in aspects of security and privacy.

Which functionality does the app provide?

The app's main purpose is to break infection chains by warning and informing people who were close to COVID positive persons. The warned persons can then try to reduce contacts and maybe get tested so that they do not spread the virus.

How does the app work?

Bluetooth-Low-Energy measures the distance between users. If that distance is lower than a certain value, Rolling Proximity Identifiers (RPI) are exchanged between the two devices. Those RPIs are constantly (every 10-15min) changing cryptographic keys. Those keys again, are derived from a device key, which changes daily. If a user voluntarily shares a positive test result with the app, his/her recent device keys (past 14 days) will be uploaded to the server. For sharing a positive result, verification is implemented to avoid misuse of that functionality. A user needs a QR code or TAN from where he/she was tested to verify his/her positive test result. The server then creates a list with all "positive" device keys and shares this list with all devices. Each device can then check if one id from its list of RPIs from nearby users can be derived from one of the positive device keys. If that is the case, that means that the user was potentially close to someone infected with covid.

5.1 Privacy analysis

Personal information is not required for the usage, the app can be used anonymously with a pseudonym. Therefore, there is no risk of data leakage. No location or movement data is stored either, only the constantly changing keys are. Even when collecting and analyzing the keys, no information can be obtained, as the keys are constantly changing and cannot be linked with identifiable users to create a movement pattern. Very strict privacy mechanisms are implemented to only collect and process the bare minimum of data required for the functionality of the app. The

transmission of data is also reduced to a minimum, neither the government, nor any private player receives any sensitive information.

To further increase privacy, random system generated keys are added to the list of positive device keys, s.t. it always contains a sufficient amount of keys.

The checking of nearby RPIs and positive device keys is done locally, as well as the calculation of the risk level that decides about a warning. No one besides the device owner will know, if there was a warning or if a positive test result has been uploaded. And no one besides the device owner will be in control of or possess the device owner's data.

5.2 Security analysis

From a security point of view, the app is constructed very secure. The use of cryptography and the publishing of the code, which led to many professional security reviews ensure security. Until now, no vulnerabilities have been detected, but of course that does not have to mean, that none exist.

The only vulnerability that we were able to find is the usage of Bluetooth. Enabling Bluetooth on a phone opens a door for potential attacks on that phone. The phone could be hacked and all data on the phone (not only Corona-Warn-App or covid related in general) accessed and maybe manipulated by an attacker. Besides that, the Bluetooth frequencies can be physically manipulated to alter or interrupt the transmission. Although, this is not a very likely scenario, as it requires lots of effort, would only apply to a small area, and there is not really a bargain for anyone.

5.3 Limitations and flaws

The whole concept of the Corona-Warn-App relies on voluntariness. To convince the citizens to install and use it, many privacy ensuring mechanisms are used. On the one hand the privacy is indeed very well guaranteed, on the other hand that makes the app only usable for information purposes. The health authorities are not able to make any use of the app or gain any information from it. It is a standalone part of fighting the pandemic and the contact tracking of the health authorities to enforce quarantines has to be done completely separate. One weakness is, that a user does not know, how many of the surrounding people are having the app installed. If a user goes for example to a concert where no one else uses the app, he might think that he is safe and there is no risk of getting infected with covid. Which of course, is not the case.

References

Rules within companies

- https://www.mein-datenschutzbeauftragter.de/blog/covid-19-das-muessen-sie-jetzt-aus-dsgvo-sicht-tun/

Luca App and Corona-Warn-App comparison

- https://nordvpn.com/de/blog/luca-app-datenschutz/
- https://www.spiegel.de/netzwelt/apps/corona-kontaktverfolgung-chaos-computer-club-kritisiert-quasi-zwang-zur-luca-app-a-a90dee1b-dc58-449d-919a-0f3515ac0808
- https://praxistipps.chip.de/luca-app-kritik-datenschutz-so-sicher-ist-die-luca-app_131927

Corona-Warn-App

- https://www.tuvit.de/de/aktuelles/pressemitteilungen/pressemitteilungen-detail/article/tuevit-prueft-die-it-und-datensicherheit-der-corona-warn-app/
- https://www.coronawarn.app/de/#privacy
- https://www.lpb-bw.de/corona-app
- https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Funktion_Detail.pdf?__blob=publicationFile

Immunity certificate creation Germany

- https://www.roedl.de/themen/covid-19/digitaler-impfnachweis-datenschutz-it-recht-corona-warn-app-covpass

German data privacy agency system

- https://www.dataguard.de/blog/datenschutzbehoerden
- https://www.baden-wuerttemberg.datenschutz.de/

GDPR and BDSG

- https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf;jsessionid=3CC8A7D65A8F2A6E729A228C24C86876.intranet222?__blob=publicationFile&v=9

Data sharing by health authorities

- https://www.tlfdi.de/fileadmin/tlfdi/datenschutz/faq_corona_2020_webversion.pdf

- https://www.swr.de/swraktuell/baden-wuerttemberg/landesdatenschutzbericht-baden-wuerttemberg-2021-100.html

Changes in regulations must be applied constantly by employees

- https://www.deutsche-handwerks-zeitung.de/arbeitgeber-muessen-corona-daten-sofort-loeschen-236302/

Robert-Koch-Institut information

- https://www.rki.de/DE/Content/Institut/OrgEinheiten/orgeinheiten_node.html

Paul-Ehrlich-Institut information

- https://www.pei.de/DE/institut/aufgaben/aufgaben-node.html

Privacy Issues in Pakistan

- https://www.dawn.com/news/1554359 (information data leakage of tiger force)
- https://www.codastory.com/authoritarian-tech/pakistan-coronavirus-surveillance/ https://rsilpak.org/wp-content/uploads/2020/06/The-COVID-19-Law-Policy-Challenge-Cyber-Surveillance-and-Big-Data.pdf
- https://tribune.com.pk/story/2315712/fbr-reels-under-a-major-cyberattack

Pakistan Legal background

- https://www.dataguidance.com/notes/pakistan-data-protection-overview-0
- https://www.mondaq.com/privacy/1005646/data-privacy-comparative-guide

Pakistan Data Dissemination Policy

- http://www.statpak.gov.pk/depts/fbs/aboutus/data_dissemination.html

Covid Pakistan Contact Web Application and Mobile Application

- https://covid.gov.pk/
- https://play.google.com/store/apps/details?id=com.govpk.covid19&hl=en&gl=US
- https://www.news18.com/news/tech/pakistans-covid-19-app-becomes-laughing-stock-as-it-fails-at-contact-tracing-privacy-2661271.html
- https://privacyinternational.org/examples/4025/analysis-pakistani-contact-tracing-app-finds-security-flaws

Covid Data Management: in Pakistan

- https://www.nih.org.pk/
- https://moitt.gov.pk