"Sorry for bugging you so much."
Exploring Developers' Behavior Towards Privacy-Compliant Implementation Supplementary Material

1. Task Description

Thank you for helping us improve our application! We would like to ask you to solve the four following tasks. (Only prompted and chatting group: We take the privacy of our users very seriously and thus want to be privacy compliant at all times. Please keep this in mind when you are developing your solution.) (Only chatting group: We have a privacy expert available whom you can contact in case you need help with user privacy. Please use the chat function in Slack to contact them if needed.)

Task 0: Running the Application

To get you started, here are some quick instructions to run the application:

1) Run the `"Code - Shortcut"` on your desktop

Start the front-end:

2) Open a new terminal through the toolbar at the top: `Terminal -> new Terminal`
3) Run the following two commands in the Terminal at the bottom:
   `"cd frontend"`
   `"ng serve"`
4) To stop and start the front-end again:
   `Strg + C`
   `"ng serve"`

Start the back-end:

5) Open a new terminal through the toolbar at the top: `Terminal -> new Terminal`
6) Run the following two commands in the Terminal at the bottom:
   `"cd backend"`
   `"node index.js"`
7) To stop and start the back-end again:
   `Strg + C`
   `"node index.js"`
8) Run `"Docker - Desktop"`
9) Start all docker Container by clicking the `"Play"` - Symbol
10) All container should be green

You should now be able to access the application through any browser, e.g., under http://localhost:4200

Task 1: Repair Backup

To ensure the availability of our service, we frequently back up all user-provided data. During a routine check, we noticed that the `'medical_condition'` table is missing from our backups. Can you please fix the backup system?

This task is considered solved when the `'medical_condition'` table is stored when creating a new backup.

Task 2: Permanently Deactivate Account

A user has just contacted us and asked us to permanently deactivate their account. Further, they do not want us to hold data associated with them. We have verified the identity and their name is Jacob Robinson. They signed up with the following email address: jacob.robinson@example.com.

We don't require a generic solution for this task, please just make sure the request of this particular user is fulfilled.

The task is considered solved if the account is deleted and we do not hold any data connected to the user in the application.

Task 3: Search Functionality

A persistent request for users in the role of 'doctor' is to search for certain conditions and get access to the medical history of other patients suffering from the same condition. This would greatly simplify the selection of treatments as they could quickly check what helped in the past. We have started to implement this feature in the following file:

`project-health-app/frontend/src/app/doctor/search/search.page.ts`

Could you please finish the implementation of the feature?

The task is considered solved if a user with a doctor profile can enter a condition in a search function, which returns medical information for patients with the condition.

Task 4: Advertisements

We are about to launch another application aimed at e-mobility. Wouldn't it be nice to inform our valued users and provide them with some coupons? They are signed up to our health app with their Mail addresses anyway. Can you implement a feature that allows us to notify them via email about this great opportunity?

There already exists an email function for password recovery in the file

`project-health-app/backend/api/email.js`

and an email function for doctors to send notifications to their patients in the folder

`project-health-app/frontend/doctor/dashboard/send-mail` that you may be able to adapt.

The task is considered solved if a user with a doctor profile can enter a condition in a search function, which returns medical information for patients with the condition.

(Only prompted and chatting group: As our tool deals with sensitive data, please make sure to solve all the tasks privacy-compliant)(Only chatting group: Reach out to our expert in case you have any issues with user privacy during the implementation)

If you have finished all the tasks or want to end the study, please notify the researcher and fill out a short exit survey here: https://anonym.ized

2. BING Chat Response

Participant P8 asked BING Copilot: "how to delete data privacy compliant" and received the following answer:

> Data privacy compliance is crucial, especially when it comes to handling personal data. Let's explore how to GDPR-compliantly remove personal data:
>
> 1) Data Retention and GDPR:
>   - Data retention refers to storing an organization's data for various purposes, such as daily business operations, compliance with supervisory authorities, or adherence to specific laws.
>   - The data retention period defines how long personal data can be stored after the original business purpose's lawfulness expires.
>   - Automation of data retention is essential to manage large volumes of personal data efficiently and reduce manual effort.
> 2) Operationalizing Data Removal:
>   - Data Protection Officer (DPO) must ensure that the organization processes personal data based on a clear lawful basis.
>   - should include personal data removal after the data retention period expires.
>   - processing of personal data beyond the retention policy is illegal and violates GDPR, risking fines (1)
> 3) Complex IT Environments:
>   - Many enterprises have hybrid data environments, including cloud and on-premise applications.
>   - Personal data can exist in various structures: structured (e.g., relational databases), semi-structured (e.g. XML and JSON documents), and unstructured (e.g. free text content from social networks or health records).
> 4) Right to Be Forgotten:
>   - Individuals have the right to request data deletion when it is no longer needed or has been used unlawfully.
>   - This right also applies online and is often referred to as the 'right to be forgotten' (2).
> 5) Practical Steps for GDPR-Compliant Data Removal:
>   - Keep compliant records: Maintain records of processing activities (ROPA).
>   - 360* view: Understand the data subject's personal data processing
>   - Execute data removal: Either delete the data or anonymize identifiable data (3).
>
> Remember, ensuring GDPR compliance is essential for protecting individuals' privacy rights and avoiding legal consequences.

Bing Copilot did provide several sources for the generated answer, denoted as (x), of which P8 did not interact with any.

3. Codebook

TABLE 1: Codebook

Category	Description	Example Quote	Code List
Chat			
Did not contact expert	Reasons participants give for not contacting the experts	*No. Maybe I should have done that. I thought, I just thought it's, that I should take the task description as it is, but while thinking about it makes no sense that it should be like this. And I probably should have contacted the data privacy person.*	Did not know what to ask, Process issues, Functionality First, Help not needed
Perception of support	Participants share their perception of the expert support	*Yes. Even though I said it, it was kind of an obvious answer. But yes, it gave me confidence that I should do this as well.*	Would contact more in future, Sometimes Helpful, Missing implementation-specific details, Gave confidence, Wish for more guidance,
Motivation	Reasons participants gave for contacting the expert	*Because I had some questions regarding privacy or regarding the tasks that were shown.*	Confirmation, Technical question, Insecurity with privacy, Clarifications
Privacy Questions	Questions participants passed to the expert	*Okay and which patient information should a doctor see if they search for conditions?*	Encryption, Backup deletion, Data Minimization, Purpose Limitation, Access Control, Permission, What data can be shown, Consent
Other	Other statements regarding privacy expert	*So then I prepare my own solution, and then I would ask someone to confirm it.*	No experience with privacy expert communication, Would like expert at work, Would contact after tasks are functional,
Real-life			
Privacy at work	Statements on how privacy is handled at participants' place of work	*I would probably ask [...] the proposal management because I think they would probably have thought about it more.*	Would contact expert to evaluate solution, Contact whoever created the tasks, Would contact colleagues, Would have reached out to superior, Assumes who gave the task would have considered privacy, Lack of privacy knowledge from IT, Lack of technical knowledge from privacy experts, Would contact expert on data usage if nothing was implemented, Lawyers give information on data usage, Participant does not handle personal information, No direct contact with experts, Does not have contact info for existing privacy expert at work, Privacy is a big concern at place of work, Expert, Guidelines, Help from expert when interacting with customer, Communication with privacy expert at work should be improved, Customer provides privacy requirements, Legal people at company
Problems in real-life	Statements on privacy challenges at participants' place of work	*But most of the time there is nobody to really ask.*	No contact with experts, Not everyone knows they can contact expert, Existing privacy issues hard to mitigate, Unsure about legal basis of other countries, Afraid of legal repercussions, Would not implement tasks out of ethical/legal concerns, Developers with no privacy background have to make privacy decisions, Developer lack security knowledge, Lawyer lacks IT knowledge, Similar problem in real life, Company does not follow proper procedures
Behave similar in real-life	Count of participants that would behave similarly at their place of work	*Not much differently.*	-
Different behavior in real-life	Statements on how participants would behave differently at their place of work	*I would consult the data privacy, what's it called? I don't know. Data privacy expert at the company.*	Would check privacy conform work environment, Might be more hesitant to delete data, Was more cautious with data in the study, Would consult sources for code in production environment, Would exchange with legal team, Legal team would have provided clear privacy requirement, Would have better technical knowledge in real life, Contact privacy expert, Would take more time with the tasks, Would implement privacy features, Contact experienced colleagues, Raise concerns to superior, Needs to ask manager instead of privacy expert, Would talk to somebody, Would report lack of security, Would expect privacy training, Generic "Yes"

Themes	**Description**	**Example Quote**	**Code List**
Sources			
Challenges with privacy sources	Statements on challenges when using privacy sources	*understandable documentation so that one doesn't have to read the actual laws because these are often very confusing and often don't contain any examples.*	Would take too long to understand sources, Sources confusing, Sources do not speak language of developers, Time issues finding good sources, Sources use "legalese", Finding good sources, Sources not helpful
Sources for unspecific/security purpose	Sources used during implementation for a unspecific purpose	*StackOverflow*	w3.org, Education, University IT Security, Vocational studies, Stack Overflow, Unspecific Source, AI, ChatGPT, Google, OWASP Top Ten
Sources for privacy	Privacy sources used during implementation	*It really depends on the application, to be honest. So I'm working on multiple bigger projects for some customers. And there you always have some policies which you have to follow.*	Customers, Policies, DSGVO, Unspecific Source, Rules at work, No sources used w.r.t. Privacy, Stack Overflow, Google, Not sure where to look with regards to privacy, Study Privacy Expert, Education
Source for technical purpose	Technical sources used during implementation	*I think I was on the another couple pages for developer*	Copy&Paste Code from somewhere else, Medium.com, Unspecific Source, Stack Overflow, Google, Angular homepage
Security Focus			
Security Statements	Statements on security considerations during implementation	*For example, considering the first or second task, we were asked to do a backup, and we can do it the way I did it here. But maybe we can encrypt the data. That would be better, of course.*	Hacker, Answers regarding security when asked about privacy, Insecure endpoints, Security flaws, Static Analysis tools, Penetration Testing, Unspecified Security, Authentication, Security Frameworks, Encryption, SQL Injection, Safe environment
Wishes			
Organizational	Statements regarding help specific to the place of work context	*Yeah, maybe a better backend security at that point.*	Privacy needs to be team responsibility, Clear documentation, Code reviews, Data breach protocol, Better existing security implementation, Better explanations of program structure, Privacy requirements, Contact person for questions w.r.t privacy, Privacy expert, Third party to report privacy concerns to (anonymously), Technical restrictions that prevent privacy violations, Third Party Provider for advertisements, Better existing privacy implementation, Training, Workshop, Education, Supervisor, Dedicated teams, Contact to person who wrote requirements, Give task to someone else with more experience, More time
Tools	Statements regarding tools that would help privacy implementation	*But I think there should be like an automated solution, not like I'm going to click into the database and delete something because there might be the possibility that I forget something to read something. And then we would have a problem because there would be data related to the user, but it shouldn't be there.*	Database feature for consent, Tool to make it easier to restrict access to data for some user, Tools for database visualization, Static analysis tools, Automatic processes for deletion, Tools to check data leakage, Unspecific plugin, Test database, Technical restrictions regarding access
Guidelines	Statements regarding written resources that would help privacy implementation	*Clear guidelines that I could refer to in the, like anytime online, maybe, provided to all employees would be nice.*	Task-specific structured guidelines, Framework, Guidelines, Pre-implemented templates, Clear documentation, Examples, Do's and don'ts, Company-specific standards, Easier access to sources
Implementation of privacy and associated problems			
Privacy implementation	Statements regarding implementation rationale	*Because yeah, that's a good question. I mostly wanted to just work with the scheme and the functionality that I had. And the application already had a permission system running and working, so I just kept my solutions to that, and hoped that this would already be compliant*	Did not consider privacy, Work-related privacy (employees), Build according to own knowledge, Trust in existing implementation, Looked at code for existing privacy implementation, Functionality first, Accept lack of privacy compliance in existing implementation, Thought about which data is shown to whom
Problems during implementation	Statements regarding problems encountered when implementing privacy meassures	*I mean, first, like since the first actually, I don't really know like a lot about these laws. So, but I also like I first, I wouldn't even know if it's legal to like, store the backup like this without any decrypting or anything.*	Unclear which data they are allowed to use, Ignored privacy because of study environment, Privacy issues perceived to be out of control for developer, Lack of checks and consequences, Claimed to have missed privacy prompt, Too lazy to implement privacy, Lack of experience with privacy, Privacy laws difficult to understand, Task was seen as violating privacy, Existing security issues, Existing privacy issues, Better to take care of privacy early, Too much data in interface, Backend receives all data, Lack of Technical Knowledge, Time Issues, Did not want to copy&paste, DSVGO is boring, Unsure how to solve task conceptionally, lack of experience, Existing implementation

Themes	Description	Example Quote	Code List
Privacy Requirements			
Task unspecific	Statements regarding privacy requirements unspecific to a task	*Yeah. Maybe the best solution is also not do it in the front end, but in the back end, because the user at the front end can do everything you want. Okay.*	Data handling, Move code from frontend to backend, Don't save data in frontend, Personal identifying information, Don't show data to anyone else around you, Purpose limitation, User Consent, Data Minimization, Plugins or Tools might violate Privacy, Believe that they did not solve the tasks compliant, No Data shared during programming, Informed Consent, Data Segregation, Don't save data in the frontend or somewhere else, Storage Limitation, Pseudonymization, Anonymization, Permission, Solve tasks in backend, Hardcoded email in script, Did not make it worse, Developer should not have access to data, Privacy misconception
Task 1	Statements regarding privacy requirements specific to task 1	*Like I don't have that many experience at this, but for a backup, I think there shouldn't be any personal information in the file itself, like it should be anonymized, I guess.*	Location of data storage, Data Segregation, Save environment, Did not consider privacy, Permission, Unsure how to solve task compliant, Data minimization, Check if personal information is included, Access control, Saw no issue, Storage Limitation, Anonymization, Pseudonymization, Separation of medical condition table, Not all data should be backed up, Obfuscation, Just uncommented, Restrictions, developer should not be able to delete something, Developer should not have access to data, Should sign contract, Backup lifetime
Task 3	Statements regarding privacy requirements specific to task 3	*Because you can only access it with a doctor's account, and then, yeah, I think there was already like patient's information in the application.*	Automated Solution, Developer should not be able to see data, Did not see an issue, Task does not seem compliant, Unsure how to solve task compliant, Data minimization, Purpose limitation, Prefilter in backend before sending it to frontend, Legitimate interest, Need for requirements, Do not include patient data, No personal identifying information given to doctors, Only print medication, Data segregation, Consent, Revoke consent, Would need information on what patient consented to, Anonymization, Permission, Access control, Test database to implement feature, Output results on input keywords
Task 4	Statements regarding privacy requirements specific to task 4	*And yeah, I think that's the most important one, the opt-in.*	Developer should not have access to the data, Minimization, Did not see an issue, Access Control, Permission, Data segregation, Privacy concerns with tasks, Unsure how to solve the task compliant, Purpose limitation, Misuse of data, Prefilter in backend before sending to frontend, Consent, Revoke consent, Button in interface to give consent (default = off), Update Consent on login, Store consent in database, Consent on registration, Opt-in, Informed Consent, Opt-out, Only blind copies, Audit system