BAB III

PELAKSANAAN KERJA MAGANG

3.1 Kedudukan dan Koordinasi

3.1.1 Kedudukan Kerja Magang

Selama menjalani proses magang di Bank Sahabat Sampoerna, penulis melakukan kegiatan-kegiatan berikut.

- Terkait proyek *Personal Data Protection (PDP)* yang merupakan penempatan utama penulis, penulis terlibat dalam berbagai kegiatan yang meliputi proses *kick-off* proyek, penugasan PDP Champion di setiap divisi, dan pembuatan memo biaya. Selanjutnya, penulis mengumpulkan kebutuhan dan persyaratan, seperti SOP & Kebijakan Bank Sahabat Sampoerna, Perjanjian Kerja Sama, dan Terms and Condition aplikasi terkait untuk di-*review* bersama vendor. Selain itu, penulis bersama dengan tim dan vendor juga melakukan *gap analysis* untuk SOP yang telah ada di Bank Sahabat Sampoerna terhadap regulasi PDP dan mengadakan PDP Training bagi seluruh pihak yang terkait. Setelah itu, penulis melakukan evaluasi dan *review* Playbook & Roadmap dari vendor serta mempersiapkan perangkat tata kelola dan membentuk Inventaris Data Pribadi. Penulis juga terlibat dalam melakukan Data Privacy Impact Analysis (DPIA) dan sosialisasi PDP kepada seluruh pihak di dalam perusahaan. Selain itu, penulis juga terlibat aktif dalam pembuatan *Consent Management System* dan melakukan peningkatan atau perbaikan pada 10 aplikasi *customer facing* yang terkait dengan pengembangan sistem tersebut.
- Terkait proyek Fraud Management System, penulis bertanggung jawab atas penarikan data menggunakan query dari *Operational Data Store (ODS)* dan menyediakan visualisasi data transaksi.
- Terkait proyek *Bring Your Own Device (BYOD),* penulis bertanggung jawab dalam menyusun materi migrasi platform untuk aktivitas terkait pekerjaan.

Selama magang, penulis bekerja secara langsung (*onsite*) di Sampoerna Strategic Square, kantor pusat Grup Sampoerna di Jakarta Selatan. Namun, dalam satu bulan terakhir, penulis bersama dengan tim IT Business Enablement mengalami migrasi ke KCP Wachid Hasyim.

3.1.2 Koordinasi Kerja Magang

Selama menjalani praktik sebagai pegawai magang di divisi IT Business Enablement, penulis berkoordinasi dengan Project Manager sebagai *supervisor* dan pembimbing lapangan penulis di bawah Pimpinan Unit Kerja IT Business Enablement Delivery Channel.

Dikarenakan *supervisor* penulis mengepalai proyek *Consent Management System* dan Fraud Management System, penulis bertanggung jawab terhadap kegiatan kedua proyek tersebut dan melaporkannya kepada *supervisor* penulis. Sementara untuk proyek *Bring Your Own Device (BYOD),* tugas tersebut diberikan langsung oleh Direktur Teknologi Informasi kepada penulis, sehingga penulis bertanggung jawab langsung kepada beliau untuk proyek tersebut.

3.2 Tugas dan Uraian Kerja Magang

Adapun daftar tugas dan tanggung jawab yang telah terlaksana selama penulis melakukan praktik sebagai karyawan magang pada unit kerja IT Business Enablement di Bank Sahabat Sampoerna adalah sebagai berikut.

Tabel 3. 1 Daftar Tugas dan Tanggung Jawab yang telah Terlaksana

No.		Jenis Pekerjaan	Mulai	Selesai
Onboarding dan Brainstorming Personal Data Protection (PDP)				
1	1.a	Memperkenalkan diri dan mempelajari unit kerja IT di Bank Sahabat Sampoerna	02 Januari 2024	02 Januari 2024
	1.b	Mengikuti *meeting* konsep dasar penerapan *Personal Data Protection (PDP)*	02 Januari 2024	02 Januari 2024
	1.c	Mempelajari konsep-konsep *Personal Data Protection (PDP)*, hasil konsultasi dengan konsultan, dan melakukan *brainstorming* dengan tim	02 Januari 2024	05 Januari 2024
Project Kick-off				
2	2.a	Mempelajari aliran dan penyimpanan data pada Bank Sahabat Sampoerna	08 Januari 2024	10 Januari 2024
	2.b	Membuat *data lineage* 10 aplikasi terkait	08 Januari 2024	10 Januari 2024
	2.c	Menyusun materi *project kick-off*	11 Januari 2024	19 Januari 2024
	2.d	Presentasi *project kick-off*	22 Januari 2024	22 Januari 2024
PDP Champions Assigning				

3	3.a	Merangkum tugas dan tanggung jawab *PDP Champions*	15 Januari 2024	18 Januari 2024
	3.b	Penugasan *PDP Champions*	19 Januari 2024	24 Januari 2024
Memo Biaya				
4	4.a	Menyusun memo biaya proyek *Personal Data Protection (PDP)*	25 Januari 2024	31 Januari 2024
Gathering Requirenments				
5	5.a	Mengumpulkan Standar Operasional Prosedur (SOP), kebijakan terkait keamanan informasi dan privasi data, dokumen-dokumen seperti Perjanjian Kerja Sama (PKS), Non-Disclosure Agreement (NDA), dan Terms and Condition (TnC)	01 Februari 2024	30 April 2024
	5.b	Mendaftar dan menentukan 10 aplikasi-aplikasi perbankan untuk implementasi awal	01 Februari 2024	07 Februari 2024
	5.c	Mendaftar *field* registrasi di setiap aplikasi *pilot* yang telah ditentukan	12 Februari 2024	28 Maret 2024
Gap Analysis				
6	6.a	Mengevaluasi kesenjangan antara kebijakan dan dokumen yang sudah ada di perusahaan dengan yang diharapkan sesuai regulasi	26 Februari 2024	08 Maret 2024
PDP Training				
7	7.a	Menyusun memo biaya *PDP Training*	19 Februari 2024	01 Maret 2024
	7.b	Melaksanakan *PDP Training*	04 Maret 2024	04 Maret 2024
Playbook & Roadmap				
8	8.a	Melakukan diskusi dengan vendor terkait penyusunan *playbook* dan *roadmap* yang sesuai dengan perusahaan	19 Maret 2024	30 April 2024
	8.b	Bersama dengan vendor mempresentasikan hasil *roadmap* terbentuk kepada pimpinan	27 Maret 2024	27 Maret 2024
Perangkat Tata Kelola				
9	9.a	Melakukan diskusi secara berkala dengan vendor terkait *draft* rancangan perangkat tata kelola (PKS, TnC, dan NDA)	13 Maret 2024	30 April 2024
Inventaris Data Pribadi				
10	10.a	Melakukan diskusi penyusunan *template* inventaris data pribadi dengan vendor	18 Maret 2024	22 Maret 2024
	10.b	Melakukan *briefing* kepada setiap unit kerja mengenai prosedur pengisian *template* dan meninjau hasil penyusunan inventaris data pribadi dari setiap unit kerja	25 Maret 2024	19 April 2024
Data Protection Impact Assessment (DPIA)				
11	11.a	Melakukan diskusi penyusunsn *template Data Protection Impact Assessment (DPIA)* dengan vendor	18 April 2024	19 April 2024
	11.b	Melakukan *briefing* kepada setiap unit kerja mengenai prosedur pengisian *template* dan meninjau hasil penyusunan *Data Protection Impact Assessment (DPIA)* dari setiap unit kerja	22 April 2024	30 April 2024
Consent Management System				
12	12.a	Mengikuti *pre-discussion* konsep rancangan sistem	26 Februari 2024	29 Februari 2024

	12.b	Melakukan diskusi dengan *supervisor* terkait menu-menu yang akan terdapat pada sistem	01 Maret 2024	08 Maret 2024
	12.c	Menyusun Architectural Decision Record (ADR)	13 Maret 2024	28 Maret 2024
	12.d	Mengikuti IT Solution Advisory Board (SAB)	25 Maret 2024	25 Maret 2024
	12.e	Menyusun rancangan antarmuka sistem	13 Maret 2024	30 April 2024
	12.f	Mengikuti peninjauan dan revisi hasil rancangan dengan pimpinan	24 April 2024	30 April 2024
Enhancement 10 Aplikasi *Customer Facing*				
13	13.a	Membahas gambaran *enhancement* yang akan dilakukan dengan setiap pemegang aplikasi	20 Maret 2024	28 Maret 2024
	13.b	Menyusun *Business Requirenment Document (BRD)*	20 Maret 2024	30 April 2024
Bring Your Own Device (BYOD) Project				
14	14.a	Melakukan *initial discussion* dengan pimpinan terkait konsep proyek *Bring Your Own Device (BYOD)*	01 Februari 2024	01 Februari 2024
	14.b	Menyusun materi *Bring Your Own Device (BYOD)*	02 Februari 2024	13 Februari 2024
	14.c	Mengikuti peninjauan dan revisi materi *Bring Your Own Device (BYOD)*	15 Februari 2024	16 Februari 2024
Fraud Management System Project				
15	15.a	Melakukan *query* penarikan data *Near Real Time (NRT)* dan *batch*	12 Januari 2024	30 April 2024
	15.b	Membuat visualisasi data terkait indikasi transaksi *fraud*	12 Januari 2024	20 Februari 2024
	15.c	Membuat visualisasi data jumlah transaksi dan rata-rata *delay* per jam	12 Januari 2024	30 April 2024

3.2.1 *Onboarding* dan *Brainstorming Personal Data Protection (PDP)*

Sebelum memulai proyek, pada hari pertama penulis bergabung dengan tim di Bank Sahabat Sampoerna, penulis sebagai mahasiswa magang baru di unit kerja IT Business Enablement melakukan perkenalan diri dengan anggota tim. Saat memasuki kantor untuk pertama kalinya, penulis diperkenalkan oleh supervisor kepada Pimpinan Unit Kerja IT Business Enablement Delivery Channel. Setelah itu, Pimpinan Unit Kerja IT Business Enablement Delivery Channel memperkenalkan penulis kepada seluruh anggota tim. Penulis juga berkesempatan bertemu dan memperkenalkan diri dengan seluruh tim IT di Bank Sahabat Sampoerna yang dipandu oleh supervisor.

Setelah sesi perkenalan, supervisor memberikan penulis bagan organisasi untuk membantu penulis memahami struktur divisi IT di Bank Sahabat Sampoerna beserta anggotanya. Karena lantai divisi IT sudah padat, seluruh tim IT Business

Enablement, termasuk unit kerja Delivery Channel, Business as a Service, dan Core & General Services, ditempatkan di lantai yang berbeda dan menggunakan *function room*. Penempatan di *function room* dilakukan secara bergantian dengan divisi IT Governance, Risk & Assurance setiap minggunya untuk mengatasi kepadatan karyawan.

Selama masa magang di Sampoerna Strategic Square, penulis bergantian bekerja di *function room* dan lantai IT setiap minggunya. Mulai bulan April, unit kerja IT Business Enablement dan IT Governance, Risk & Assurance tidak lagi menggunakan *function room*, tetapi bergantian untuk menggunakan kantor cabang baru yang bertempatan di Wahid Hasyim (terletak di sebelah hotel Swiss-Belin). Unit kerja IT Business Enablement mendapatkan giliran pertama untuk bekerja di kantor cabang Wahid Hasyim, sehingga sampai dengan akhir masa magang penulis, penulis bekerja dari kantor baru tersebut.

Selama masa magang ini, penulis melakukan perjalanan pulang-pergi. Untuk menuju Sampoerna Strategic Square, penulis menggunakan Kereta Api Bandara dari stasiun Batu Ceper ke stasiun BNI City (Sudirman Baru). Dari sana, penulis berjalan sekitar 1 km menuju stasiun MRT BNI City (Dukuh Atas). Kemudian, penulis menggunakan MRT untuk mencapai stasiun MRT Bendungan Hilir. Gedung Perkantoran Sampoerna Strategic Square verada tepat di depan stasiun tersebut.

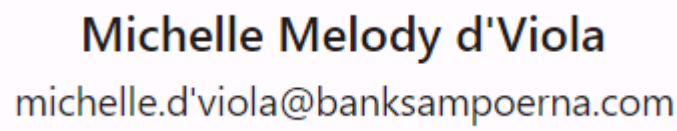
Ketika kantor berpindah ke Wahid Hasyim, rute perjalanan awal tetap sama, yaitu menggunakan Kereta Api Bandara dari stasiun Batu Ceper ke satsiun BNI City (Sudirman Baru). Kemudian, dari MRT BNI City (Dukuh Atas), penulis menggunakan MRT untuk menuju ke stasiun akhir, yaitu Bundaran HI. Dari stasiun MRT Bundaran HI, penulis berjalan sekitar 2 km untuk mencapai lokasi kantor.

Pada hari pertama, supervisor membantu penulis untuk mendapatkan akses yang diperlukan selama masa magang di Bank Sahabat Sampoerna. Salah satunya adalah kartu akses yang digunakan untuk masuk ke gedung dan mengakses lantai yang telah terdaftar. Proses permintaan kartu akses memakan waktu beberapa

minggu. Sebelum menerima kartu akses, penulis menggunakan *barcode* dengan status sebagai *visitor* yang diberikan oleh *receptionist* setiap harinya untuk masuk ke gedung dan lantai yang diizinkan.

Sebelum hari pertama penulis masuk kantor, supervisor telah membantu dalam permintaan laptop sehingga saat memulai hari pertama, penulis sudah memiliki laptop untuk bekerja. Laptop ini akan digunakan selama penulis bekerja di Bank Sahabat Sampoerna, seperti yang dilakukan oleh karyawan lainnya. Penulis dapat membawa pulang laptop ini untuk menyelesaikan tugas yang belum selesai. Setelah masa magang berakhir, laptop ini dikembalikan kepada Bank Sahabat Sampoerna.

Selain kartu akses dan laptop, supervisor juga membantu penulis untuk meminta akses akun Google Workspace kepada unit kerja IT Support. Akun ini digunakan untuk kolaborasi dalam berbagai aplikasi seperti Google Slide, Google Docs, Google Sheet, dan sebagainya, serta untuk mengorganisir dokumen dan melakukan rapat virtual menggunakan Google Meet. Penulis mendapatkan akun Google Workspace sekitar satu minggu setelah permintaan diajukan oleh supervisor. Sebelum mendapatkan akun ini, penulis menggunakan email pribadi dan harus meminta akses khusus untuk setiap dokumen yang ingin diakses. Gambar 3.1 di bawah ini menampilkan akun Google Workspace penulis.



Gambar 3. 1 Akun Google Workspace

Pada hari pertama, supervisor juga menerangkan kepada penulis mengenai *platform* yang biasanya digunakan oleh tim. Selain menggunakan Whatsapp, tim juga biasanya menggunakan *platform* bernama Slack untuk mendukung komunikasi dengan internal maupun dengan pihak eksternal seperti vendor.

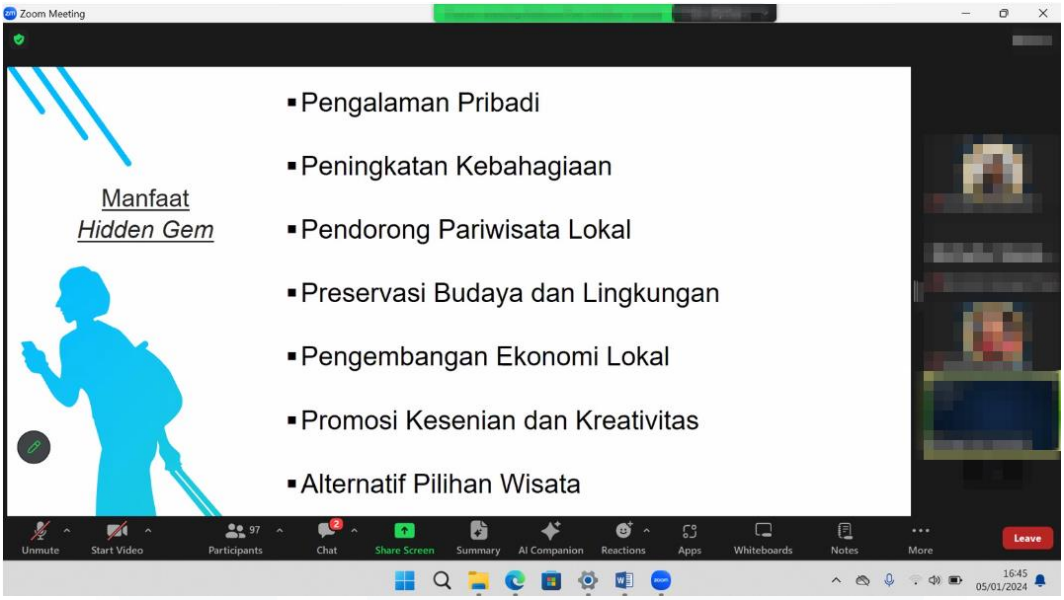
Gambar 3. 2 Logo Slack

Slack merupakan *platform* atau aplikasi komunikasi kolaboratif yang memungkinkan tim untuk berkomunikasi secara efisien dan terorganisir. Dengan menggunakan Slack, tim dapat membuat saluran (*channels*) untuk topik atau proyek tertentu, melakukan obrolan satu lawan satu, dan saling berbagi *file* dengan mudah. Fitur pencarian pada *platform* ini juga memungkinkan penggunanya untuk dengan cepat menemukan informasi yang relevan dalam obrolan-obrolan yang telah terjadi. Selain itu, Slack juga terintegrasi dengan berbagai aplikasi dan layanan lainnya, seperti Google Drive, Trello, dan Zoom, untuk meningkatkan produktivitas dan kolaborasi. Dengan tampilan antarmuka yang *user – friendly* dan berbagai fitur yang disediakan, Slack dipilih oleh tim untuk membantu proses komunikasi dan kerja sama secara efektif.

Gambar 3. 3 Logo Jira

Dalam rangka memudahkan *tracking* dan melakukan manajemen proyek, tim menggunakan *platform* Jira. Meskipun penulis tidak memiliki akses langsung ke Jira, namun penulis tetap dapat mengetahui kemajuan proyek dari supervisor berdasarkan informasi yang ada di Jira. Jira merupakan sebuah *platform* manajemen proyek yang serbaguna dan banyak digunakan oleh tim pengembangan *software* dan industri teknologi. Dengan Jira, tim dapat melacak proyek-proyek yang dijalankan dari awal hingga akhir dengan cara yang terstruktur dan terorganisir. *Platform* ini menyediakan berbagai fitur, seperti pelacakan tugas, manajemen *backlog* (daftar *task* yang perlu dipenuhi dalam sebuah proyek), pembuatan laporan, dan pelacakan *bug*, yang memungkinkan tim untuk mengelola proyek dengan lebih efisien. Jira juga mendukung berbagai metodologi pengembangan, seperti Agile dan Scrum, sehingga dapat disesuaikan dengan kebutuhan tim. Dengan tampilan antarmuka yang mudah dipahami dan kemampuan *platform* untuk berintegrasi dengan berbagai *tools* lainnya, Jira menjadi solusi yang kuat untuk manajemen proyek di berbagai industri.

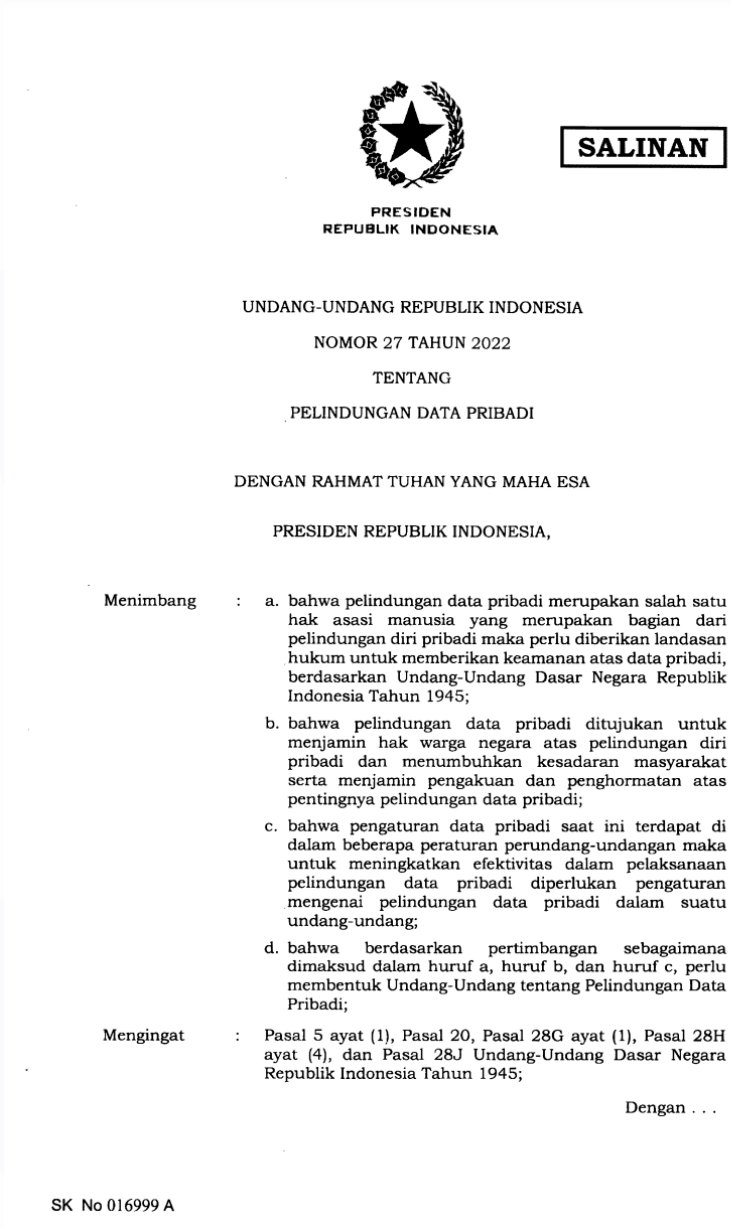
Selama menjalankan magang di divisi IT, penulis mengikuti kegiatan yang bernama IT Sharing Session yang diadakan melalui Zoom Meeting seperti pada Gambar 3.4. Kegiatan ini melibatkan tiga kelompok, masing-masing terdiri dari dua orang yang dipilih secara acak, untuk menyajikan materi terkait isu-isu sosial seperti *work – life balance*, *stress*, *toxic masculinity*, dan lain-lain. Setelah sesi presentasi, terdapat sesi tanya – jawab, kuis, dan pemilihan presenter – presenter untuk kegiatan berikutnya. IT Sharing Session diadakan setiap dua minggu sekali dengan tujuan meningkatkan kesadaran karyawan tentang isu-isu sosial yang ada di lingkungan kerja dan memberikan pemahaman tentang cara mengatasinya.



Gambar 3. 4 *IT Sharing Session*

Pada minggu pertama, penulis bersama dengan tim inti internal IT Business Enablement yang berfokus pada proyek Personal Data Protection mempelajari regulasi serta peraturan-peraturan terkait Perlindungan Data Pribadi. Hal ini meliputi peraturan umum seperti UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (seperti yang ditampilkan pada Gambar 3.5), UU Nomor 11 Tahun 2008 sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik. Adapun peraturan sektoral yang dipelajari oleh penulis sebelum proyek dijalankan adalah POJK No.1/POJK.07/2013 tentang Perlindungan Konsumen Dalam Sektor Jasa Keuangan, POJK No.6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, PBI No. 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, Surat Edaran BI No. 7/25/DPNP/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah, dan Surat Edaran OJK No.

14/SEOJK. 07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.



PRESIDEN
REPUBLIK INDONESIA

SALINAN

UNDANG-UNDANG REPUBLIK INDONESIA

NOMOR 27 TAHUN 2022

TENTANG

PELINDUNGAN DATA PRIBADI

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :

a. bahwa pelindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b. bahwa pelindungan data pribadi ditujukan untuk menjamin hak warga negara atas pelindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi;

c. bahwa pengaturan data pribadi saat ini terdapat di dalam beberapa peraturan perundang-undangan maka untuk meningkatkan efektivitas dalam pelaksanaan pelindungan data pribadi diperlukan pengaturan mengenai pelindungan data pribadi dalam suatu undang-undang;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu membentuk Undang-Undang tentang Pelindungan Data Pribadi;

Mengingat : Pasal 5 ayat (1), Pasal 20, Pasal 28G ayat (1), Pasal 28H ayat (4), dan Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Dengan . . .

SK No 016999 A

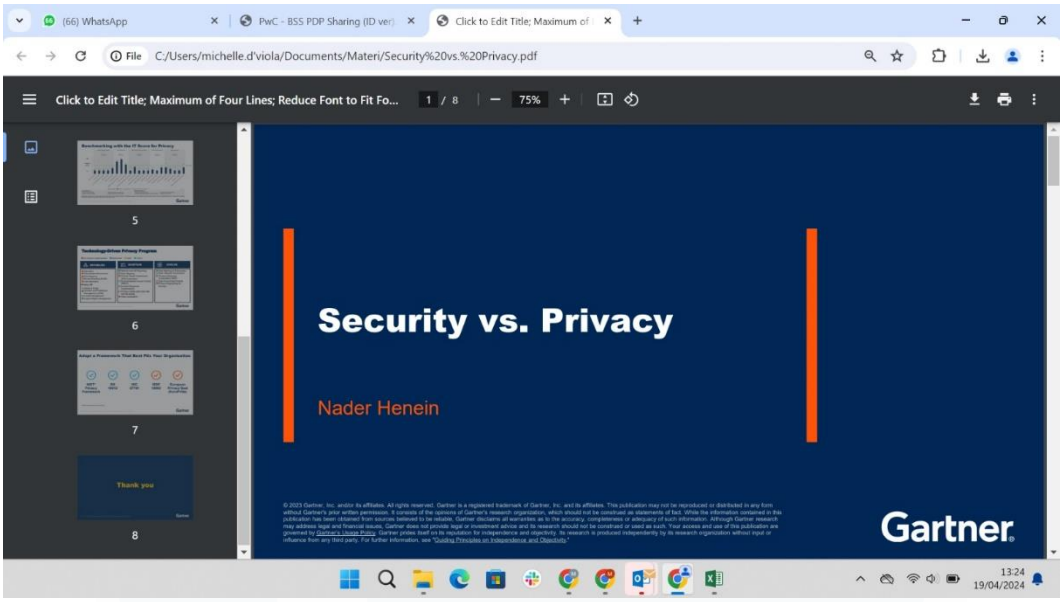
Gambar 3. 5 Undang-undang Perlindungan Data Pribadi

Selain itu, tim bersama dengan Direktur Information Technology juga mengikuti seminar dan berkonsultasi dengan beberapa konsultan luar seperti PwC dan Gartner. Dalam konsultasi dengan PwC Indonesia, tim dibantu untuk memahami konsep dan penerapan perlindungan data pribadi menurut regulasi di

Indonesia, terutama Undang-Undang Perlindungan Data Pribadi dalam bentuk *slides* seperti pada Gambar 3.6 berikut.

Gambar 3. 6 Konsultasi Perlindungan Data Pribadi dengan PwC

Sementara itu, Gartner adalah konsultan internasional yang berbasis di Stamford, Connecticut, Amerika Serikat. Konsultasi dengan Gartner memungkinkan tim untuk mendalami pemahaman tentang implementasi Perlindungan Data Pribadi dengan merujuk pada regulasi serupa di Uni Eropa, yang dikenal sebagai General Data Protection Regulation (GDPR). Adapun materi atau hasil konsultasi dengan Gartner juga dibuat dalam bentuk *slides* seperti pada Gambar 3.7 berikut.

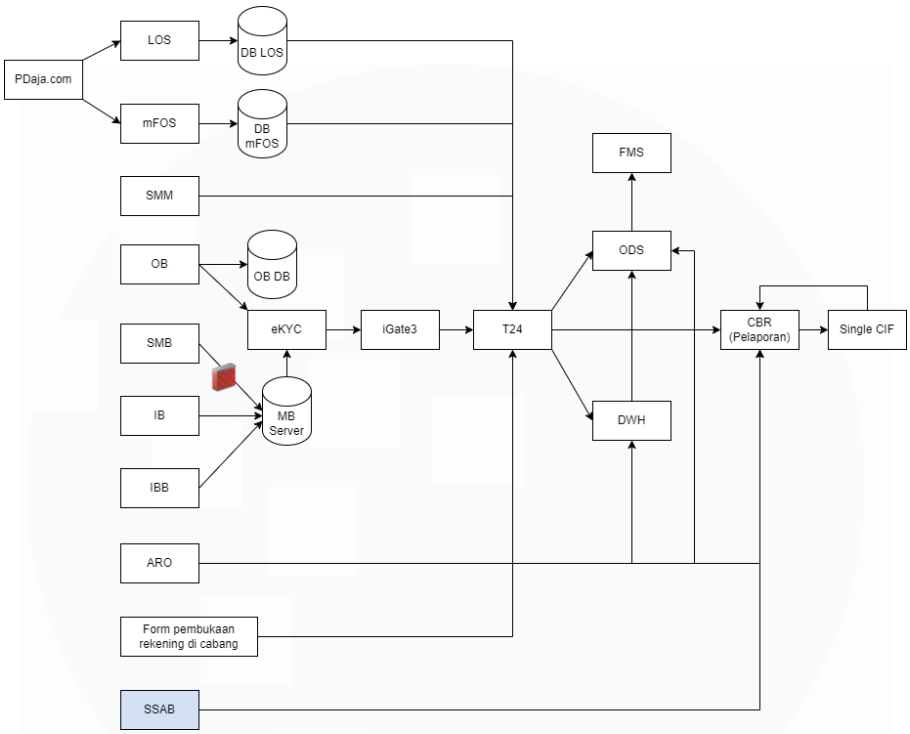


Gambar 3. 7 Konsultasi Perlindungan Data Pribadi dengan Gartner

Setelah mempelajari materi dan hasil konsultasi, tim melakukan *brainstorming* internal untuk memastikan pemahaman dan persepsi yang sama mengenai implementasi Perlindungan Data Pribadi. Hal ini merupakan hal yang penting karena aturan ini baru diterapkan di Indonesia dan perlu diikuti oleh perusahaan untuk mematuhi regulasi yang berlaku.

3.2.2 Project Kick-off

Setelah mempelajari materi yang relevan, penulis dan tim mengalokasikan waktu untuk memahami secara mendalam tentang Critical Data Elements (CDE), data governance, data lineage, dan Record of Processing Activities (RoPA). Selain itu, penulis bersama dengan tim juga mempelajari secara cermat aliran dan penyimpanan data pada Bank Sahabat Sampoerna untuk memperoleh pemahaman yang komprehensif tentang konteks proyek. Sebagai salah satu bagian dari proses pemahaman ini, penulis ditugaskan untuk menyusun bagan yang menggambarkan rancangan *data lineage* Bank Sahabat Sampoerna untuk memudahkan analisis lebih lanjut yang akan dilakukan. Gambar 3.8 berikut menunjukkan aplikasi-aplikasi *pilot* beserta alur data dari aplikasi tersebut sampai kepada sistem *core banking* yang dimiliki bank saat ini.



Gambar 3. 8 Diagram Alur Data Aplikasi *Pilot*

Adapun Gambar 3.9 berikut menunjukkan *field* data beserta contoh data pribadi yang akan dialirkan berdasarkan diagram alur data. Gambar berikut disamarkan untuk keperluan privasi perusahaan.

Gambar 3. 9 Data Lineage 10 Aplikasi *Pilot*

Setelah pemahaman dasar terbentuk, tim bekerja sama dengan tim Operational Risk beserta Data Protection Officer (DPrO) yang merupakan bagian dari tim Operational Risk yang ditunjuk untuk berkolaborasi dalam mengelola proyek ini untuk menyusun materi *kick-off meeting*. Diskusi intensif juga dilakukan dengan vendor terkait untuk memastikan pemahaman yang sama, memperoleh inspirasi, dan penyusunan materi *kick-off meeting* yang akan dilakukan tersebut. Materi ini mencakup penjelasan tentang latar belakang aturan, konsep data pribadi, pencapaian terkait tahun sebelumnya, cakupan proyek pada tahun berjalan, serta pengenalan *project charter*.

Setelah melalui beberapa tahap revisi dan diskusi materi dengan direktur Information Technology, materi *kick-off* proyek dipresentasikan kepada para pemangku kepentingan utama atau yang disebut dengan BoM - SMT (Board of Management dan Senior Management Team). Setelah hasil presentasi ditinjau oleh ORM Head, IT Business Enablement Head, Enterprise Risk, Analytic, & Control Division, serta disetujui oleh Chief SM & High End Business, Chief Digital Business, Chief Credit Officer, Chief Operations Officer, Chief Human Capital

Officer, Chief Internal Audit, ESME Business Director, Finance & Business Planning Director, Information Technology Director, Compliance & Risk Director, dan President Director, proyek secara resmi dapat mulai dijalankan.

3.2.3 PDP Champion Assigning

Dalam tahap ini, tim *Personal Data Protection (PDP)* memberikan tugas kepada setiap unit kerja di perusahaan untuk menunjuk satu orang wakil yang dianggap mampu untuk menjadi perwakilan yang bertanggung jawab atas pengelolaan data pribadi di unit kerjanya. Untuk memilih anggotanya, tim menyediakan daftar tugas dan wewenang umum dari unit kerja yang akan dipilih, berdasarkan peraturan yang berlaku serta disesuaikan dengan sebuah kebijakan yang sedang disusun oleh unit kerja Auditor, yang disebut Kebijakan Pengamanan Informasi. Karyawan yang terpilih akan menjabat sebagai PDP Champion.

Gambar 3. 10 *PDP Champion Assigning*

Proses pemilihan PDP Champion tersebut di-*blast* oleh tim internal secara langsung kepada seluruh anggota unit kerja yang bersangkutan. Proses tersebut dilakukan melalui *platform* Outlook seperti pada Gambar 3.10 (gambar tersebut disamarkan untuk keperluan privasi perusahaan), yang merupakan aplikasi *email* dan kalender yang umum digunakan di perusahaan Bank Sahabat Sampoerna untuk komunikasi internal.

Gambar 3. 11 Logo Outlook

Outlook memudahkan penyebaran informasi kepada seluruh anggota tim secara efisien dan dapat diakses dari berbagai perangkat, termasuk komputer *desktop*, *laptop*, *tablet*, dan *smartphone*. Selain itu, Outlook juga menyediakan fitur-fitur kolaborasi seperti pengaturan rapat, berbagi *file*, dan manajemen tugas yang mempermudah koordinasi dan kerjasama antar anggota tim.

3.2.4 Memorandum Biaya

Setelah menerima proposal dari para vendor, tim memulai penyusunan memorandum biaya seperti pada Gambar 3.12 yang disamarkan untuk keperluan privasi perusahaan. Memorandum biaya tersebut ditujukan kepada Board of Management. Memo tersebut mencakup beberapa aspek penting, termasuk latar belakang proyek, tujuan proyek, perbandingan antara vendor yang berbeda, estimasi biaya yang dibutuhkan, serta rekomendasi dan keputusan yang diusulkan oleh tim.

Gambar 3. 12 Memo Biaya Proyek *Personal Data Protection (PDP)*

Salah satu poin penting dalam memorandum biaya ini adalah keputusan tim setelah mempertimbangkan proposal dari berbagai vendor. Tim memutuskan untuk melibatkan satu vendor tertentu untuk membantu dalam penyusunan dokumen-dokumen terkait agar sesuai dengan ketentuan pada regulasi Perlindungan Data Pribadi (PDP). Sementara itu, terkait dengan pengembangan *Consent Management System*, tim merekomendasikan menolak proposal dari vendor *software* karena pertimbangan anggaran, dan mengandalkan sumber daya internal dari tim Bank Sahabat Sampoerna.

3.2.5 Gathering Requirenments

Dalam menunggu persetujuan memo biaya dari Board of Management dan Senior Management Team (BoM – SMT), tim memulai pengumpulan persyaratan

yang diperlukan untuk kelancaran proyek. Hal ini dilakukan sebagai upaya persiapan, terutama dalam menyediakan informasi yang diperlukan oleh vendor agar mereka dapat memulai pekerjaan.

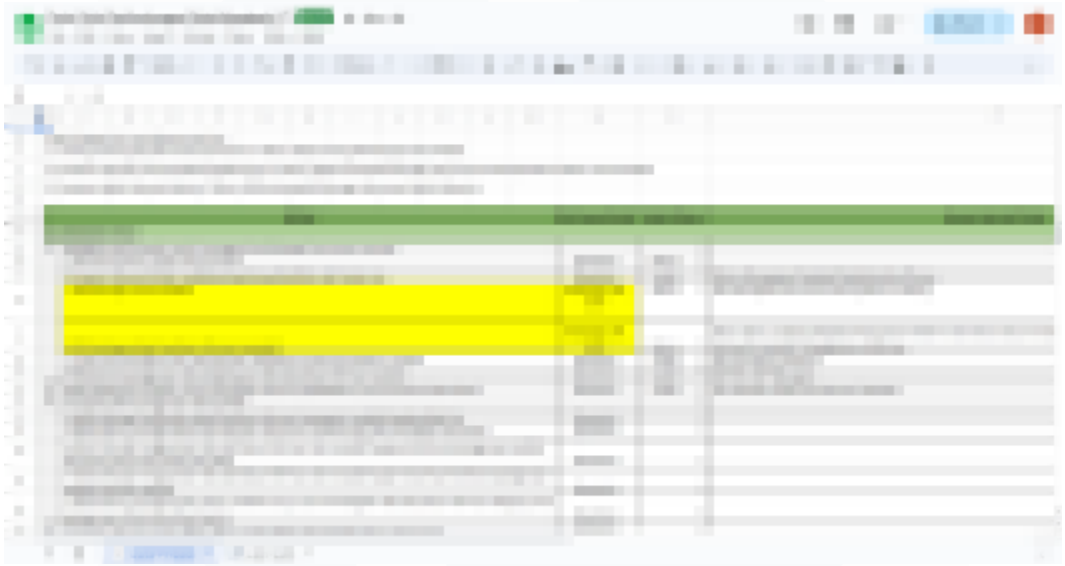
Tim telah mengumpulkan dan mencatat daftar produk aplikasi perbankan Bank Sahabat Sampoerna, yang akan digunakan untuk menentukan aplikasi mana yang akan menjadi pilot. Setelah ditentukan, dicatat *field* registrasi apa saja yang terdapat pada setiap aplikasi tersebut untuk mengetahui data pribadi apa saja yang dikumpulkan dari proses registrasi setiap aplikasi. Selain itu, tim juga telah mengumpulkan standar operasional prosedur (SOP), kebijakan terkait keamanan informasi dan privasi data, serta dokumen-dokumen seperti Perjanjian Kerja Sama (PKS), Non-Disclosure Agreement (NDA), dan Terms and Condition (TnC) terkait produk aplikasi perbankan Bank Sahabat Sampoerna. Langkah-langkah ini dimaksudkan untuk mendukung vendor dalam menyusun proposal, agar setelah disetujui oleh Bank Sahabat Sampoerna, dapat memungkinkan vendor untuk memulai pekerjaannya.

3.2.6 Gap Analysis

Untuk melakukan *gap analysis* yang bertujuan mengevaluasi kesenjangan antara kebijakan dan dokumen perusahaan dengan yang diharapkan sesuai regulasi, tim bekerja sama dengan vendor dalam menyusun *template* menggunakan format Google Sheets seperti pada Gambar 3.13. Gambar tersebut disamarkan karena mengandung informasi yang bersifat rahasia dan melibatkan privasi perusahaan. Template tersebut mencakup poin-poin penting yang terkait dengan setiap unit kerja, mengacu pada regulasi seperti Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Peraturan Otoritas Jasa Keuangan (POJK) Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan, serta Peraturan Bank Indonesia Nomor 3 Tahun 2023 tentang Perlindungan Konsumen Bank Indonesia.

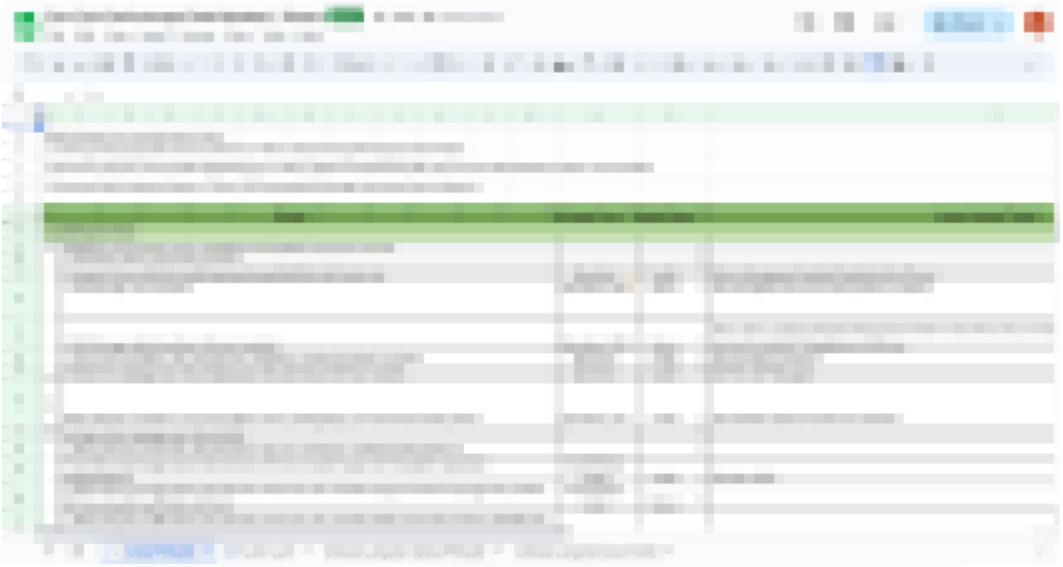
Tim, tiap unit kerja, dan vendor melakukan diskusi dan peninjauan terhadap setiap poin dalam *template* untuk menentukan apakah sudah diatur dalam kebijakan perusahaan. Jika sudah, nama aturan internal dan dokumen terkait dicatat. Tim

internal *Personal Data Protection (PDP)* bersama vendor kemudian berdiskusi untuk menentukan apakah ada kebutuhan untuk menyesuaikan aturan internal yang ada.



Gambar 3. 13 *Gap Analysis* Proyek *Personal Data Protection (PDP)*

Hasil dari peninjauan tersebut dikumpulkan dalam satu folder untuk memudahkan pengorganisasian. Gap analysis dilakukan untuk seluruh unit kerja, yang meliputi Credit & Credit Policy, Operation, Legal, Information Technology, Finance, ESME Sales and Performance Management, ESME Credit, Compliance, Collection, CCIR, CAC, dan Lending Center. Dari hasil peninjauan tersebut, dibuat rangkuman gap analysis yang dikategorikan berdasarkan kategori peraturannya seperti pada Gambar 3.14.

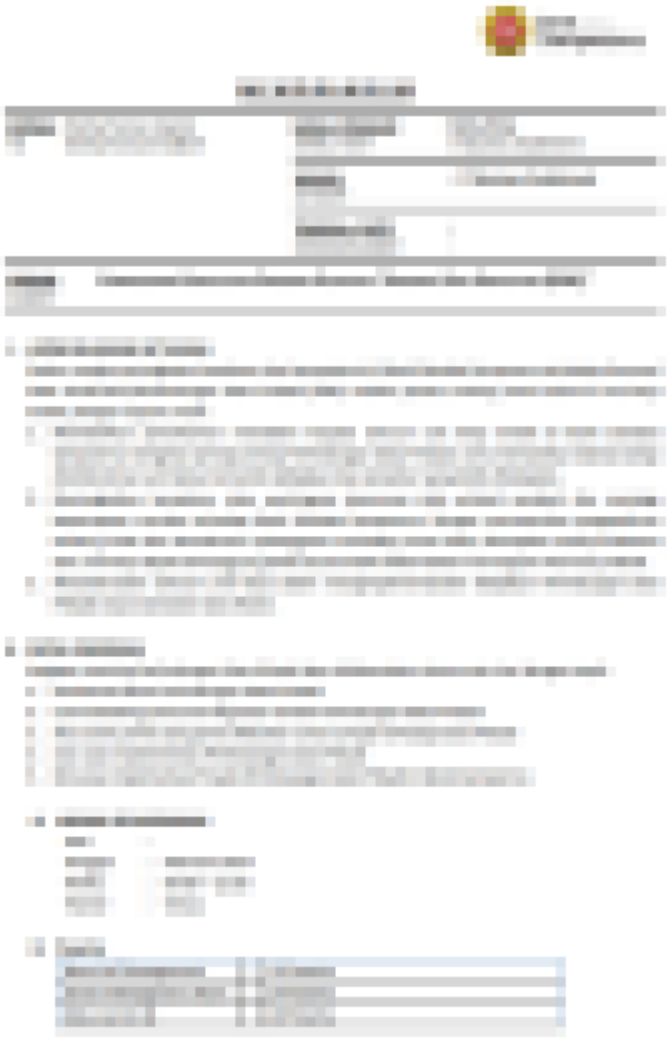


Gambar 3. 14 *Recap Gap Analysis* Proyek *Personal Data Protection (PDP)*

3.2.7 PDP Training

Dalam upaya meningkatkan kesadaran setiap unit terkait dan seluruh bagian dari perusahaan terhadap perlindungan data pribadi, tim mengadakan *Personal Data Protection (PDP)* Training. Inisiatif untuk menyelenggarakan kegiatan ini muncul dalam diskusi dengan direktur Information Technology yang menyoroti urgensi dan pentingnya pelatihan tersebut.

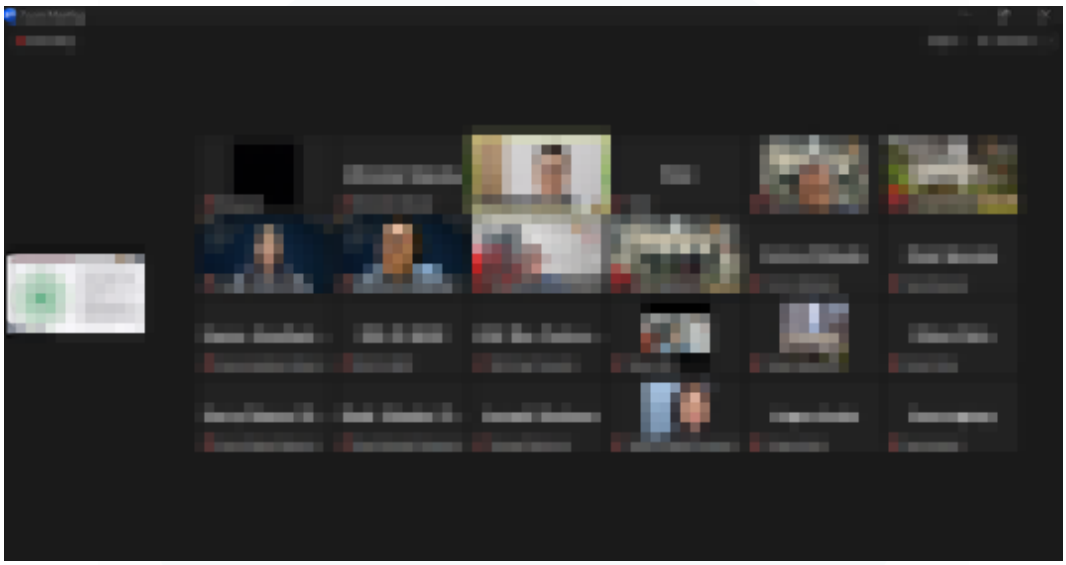
Setelah keputusan untuk mengadakan pelatihan ini diambil, tim mulai menyusun memorandum biaya yang diperlukan seperti pada Gambar 3.15. Memorandum biaya ini disusun untuk menguraikan kebutuhan anggaran yang dibutuhkan untuk pelatihan.



Gambar 3. 15 Memo Biaya *Personal Data Protection (PDP) Training*

Pelatihan ditujukan kepada seluruh *Personal Data Protection (PDP)* Champion. Materi pelatihan disampaikan oleh vendor dan dilaksanakan secara daring melalui Zoom *meeting* dengan durasi sekitar dua jam seperti pada Gambar 3.16 (gambar disamarkan karena menampilkan data pribadi karyawan perusahaan). Tujuan dari pelatihan ini adalah untuk meningkatkan kesadaran setiap *Personal Data Protection (PDP)* Champion tentang perlindungan data pribadi, mengingat hal ini merupakan hal yang baru di lingkungan perusahaan, bahkan di seluruh Indonesia. Selain itu, pelatihan juga bertujuan untuk memastikan bahwa setiap

Champion memahami peran dan tanggung jawabnya sebagai *Personal Data Protection (PDP)* Champion.



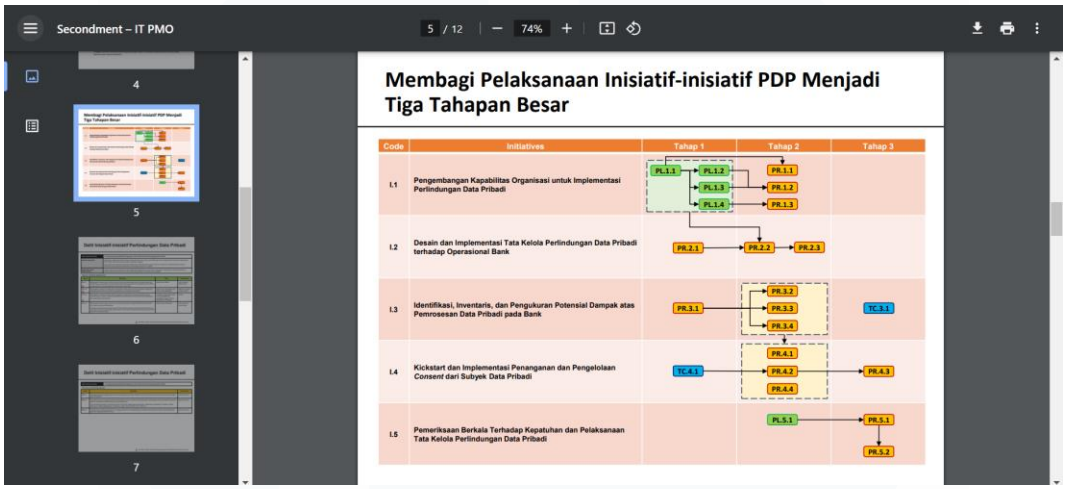
Gambar 3. 16 *PDP Training*

3.2.8 Playbook & Roadmap

Playbook & Roadmap merupakan bagian dari strategi pelaksanaan yang dirancang untuk mengarahkan langkah-langkah praktis yang diperlukan dalam implementasi kebijakan dan prosedur Perlindungan Data Pribadi (PDP). Playbook mencakup serangkaian panduan dan rekomendasi praktis yang dapat digunakan oleh berbagai unit kerja dalam perusahaan. Selama penulis menjalankan magang di Bank Sahabat Sampoerna, playbook masih dalam proses pembuatan oleh vendor. Secara garis besar, *playbook* yang dihasilkan akan berbentuk dokumen yang mencakup alur-alur tindakan yang harus dilakukan, namun tidak seformal Standar Operasional Prosedur (SOP).

Di sisi lain, *roadmap* berperan sebagai alat untuk memberikan pandangan menyeluruh tentang tahapan-tahapan pelaksanaan kebijakan PDP dari awal hingga akhir, termasuk penugasan tanggung jawab, tahap pelaksanaan, serta inisiatif-inisiatif Perlindungan Data Pribadi (PDP). *Roadmap* menjadi landasan penting bagi seluruh tim untuk memahami, mengimplementasikan, dan mengawasi kepatuhan seluruh unit kerja pada perusahaan terhadap regulasi Perlindungan Data Pribadi dengan efektif dan efisien. Sama halnya dengan *playbook*, penyusunan *roadmap*

juga dibantu oleh vendor dengan melakukan diskusi untuk mencapai kesepakatan isi dari *roadmap* tersebut dengan tim internal. Adapun cuplikan dari *roadmap* yang tersusun dalam bentuk *slides* adalah seperti pada Gambar 3.17 berikut.



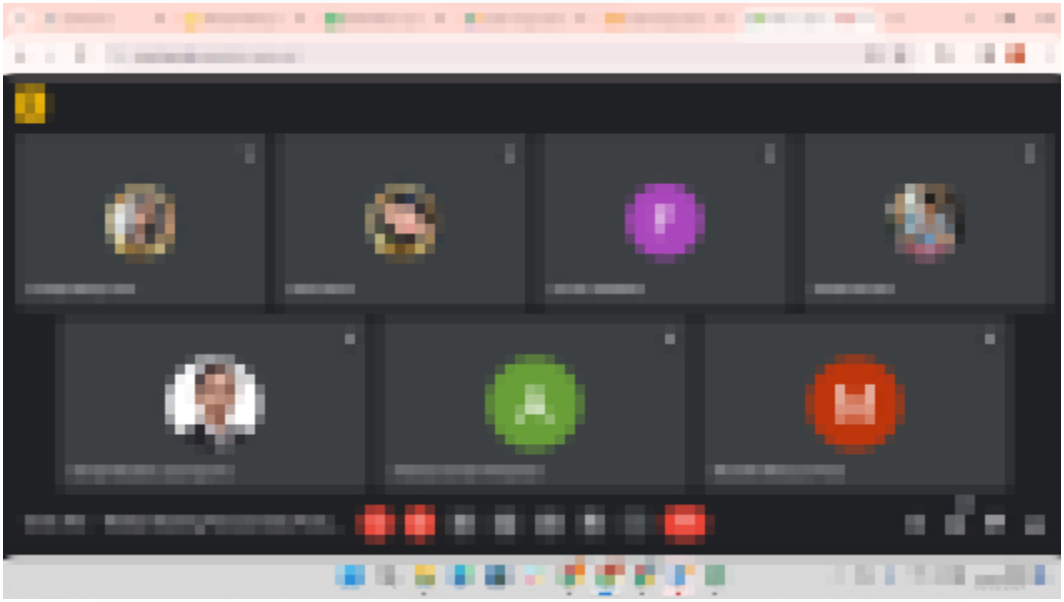
Gambar 3. 17 *Roadmap Personal Data Protection (PDP)* Bank Sahabat Sampoerna

3.2.9 Perangkat Tata Kelola

Perangkat tata kelola adalah seperangkat mekanisme yang dirancang dan diimplementasikan untuk mengelola dan mengatur berbagai aspek operasional, kebijakan, dan praktik atau kegiatan pemrosesan dalam suatu perusahaan. Perangkat ini meliputi berbagai dokumen dan kebijakan yang digunakan untuk mengatur berbagai aktivitas, prosedur, dan interaksi di dalam dan di luar perusahaan.

Dalam konteks perlindungan data pribadi pada Bank Sahabat Sampoerna, perangkat tata kelola mencakup Standar Operasional Prosedur (SOP), Kebijakan, Perjanjian Kerja Sama (PKS), Non-Disclosure Agreement (NDA), dan Terms and Condition (TnC). Vendor berperan dalam membantu tim dalam pembuatan dan penyesuaian perangkat tata kelola yang sudah ada. Tim, di sisi lain, memiliki peran yang lebih dominan dalam tahap *gathering requirenments* sebelumnya, di mana tim membantu menghimpun kebijakan serta Standar Operasional Prosedur (SOP), Perjanjian Kerja Sama (PKS), Non-Disclosure Agreement (NDA), dan Syarat dan Ketentuan (TnC) terkait perlindungan data pribadi dari setiap unit kerja untuk ditinjau oleh vendor.

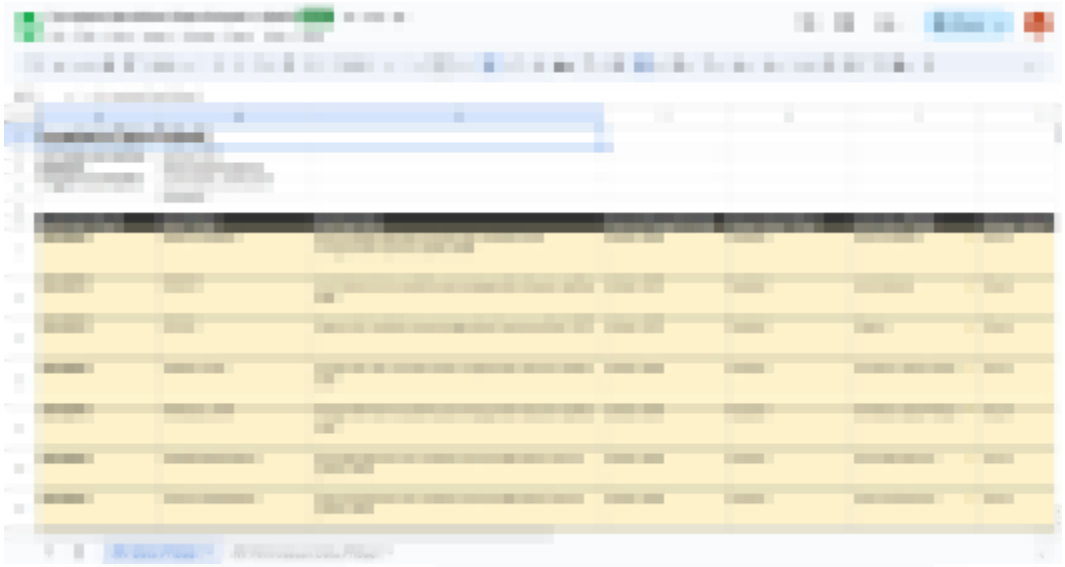
Selama proses ini, tim dan vendor secara berkala melakukan diskusi mengenai hasil dari rancangan yang telah disusun. Selama pelaksanaan proyek Personal Data Protection ini, tim bersama dengan vendor juga mengadakan pertemuan mingguan seperti pada Gambar 3.18 untuk menyampaikan permintaan, persyaratan, dan pembaruan kemajuan masing-masing, sehingga dapat saling terkoordinasi dan mengetahui kemajuan proyek.



Gambar 3. 18 *Weekly Meeting Personal Data Protection (PDP)*

3.2.10 Inventaris Data Pribadi

Untuk mengelola dan melacak setiap data pribadi dan pemrosesannya, tim bekerja sama dengan vendor untuk menyusun *template* dalam bentuk Google Sheets seperti pada Gambar 3.19. *Template* ini akan digunakan untuk menyimpan dan melacak data pribadi dari setiap proses yang dilakukan oleh setiap unit kerja sebagai bentuk dari pemenuhan peraturan atau regulasi perlindungan data pribadi yang mengharuskan perusahaan di Indonesia untuk memiliki catatan mengenai seluruh aktivitas pemrosesan data yang dilakukan oleh perusahaan atau yang disebut dalam Undang-undang dengan nama Record of Processing Activities (RoPA).



Gambar 3. 19 Inventaris Data Pribadi Bank Sahabat Sampoerna

Agar setiap unit kerja dapat memahami dan mengisi *template* dengan baik, tim internal *Personal Data Protection (PDP)* mengadakan rapat dengan masing-masing unit kerja untuk menyesuaikan *template*. Setelah *template* final telah disusun, akan diserahkan kepada tiap unit kerja untuk diisi.

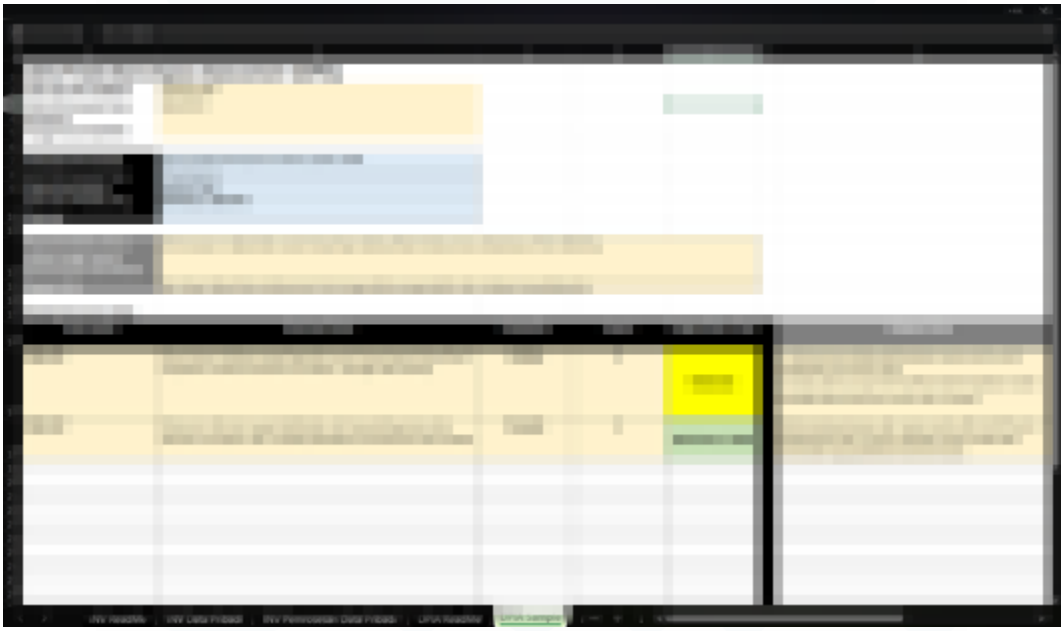
Pada dasarnya, setiap unit kerja diminta untuk melengkapi tiga hal: inventaris proses kerja, yang menggambarkan kegiatan yang dilakukan oleh unit kerja dalam setiap proses; inventaris data pribadi, yang mencakup data pribadi apa yang dipegang oleh unit kerja tersebut; dan inventaris pemrosesan data pribadi, yang menjelaskan jenis pemrosesan data pribadi yang terkait beserta data pribadi yang diprosesnya. Inventaris ini bertujuan untuk memastikan bahwa semua data pribadi yang dipegang dan diproses oleh setiap unit kerja tercatat secara terperinci dan terdokumentasi dengan baik.

3.2.11 Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessment (DPIA) adalah sebuah evaluasi untuk menilai potensi dampak suatu kegiatan terhadap perlindungan data pribadi. Tujuan utamanya adalah untuk mengidentifikasi, memahami, dan mengurangi risiko terkait privasi data sebelum memulai suatu pemrosesan. Dengan melakukan Data Protection Impact Assessment (DPIA), perusahaan dapat mengidentifikasi langkah-langkah yang perlu diambil untuk memastikan kepatuhan terhadap regulasi

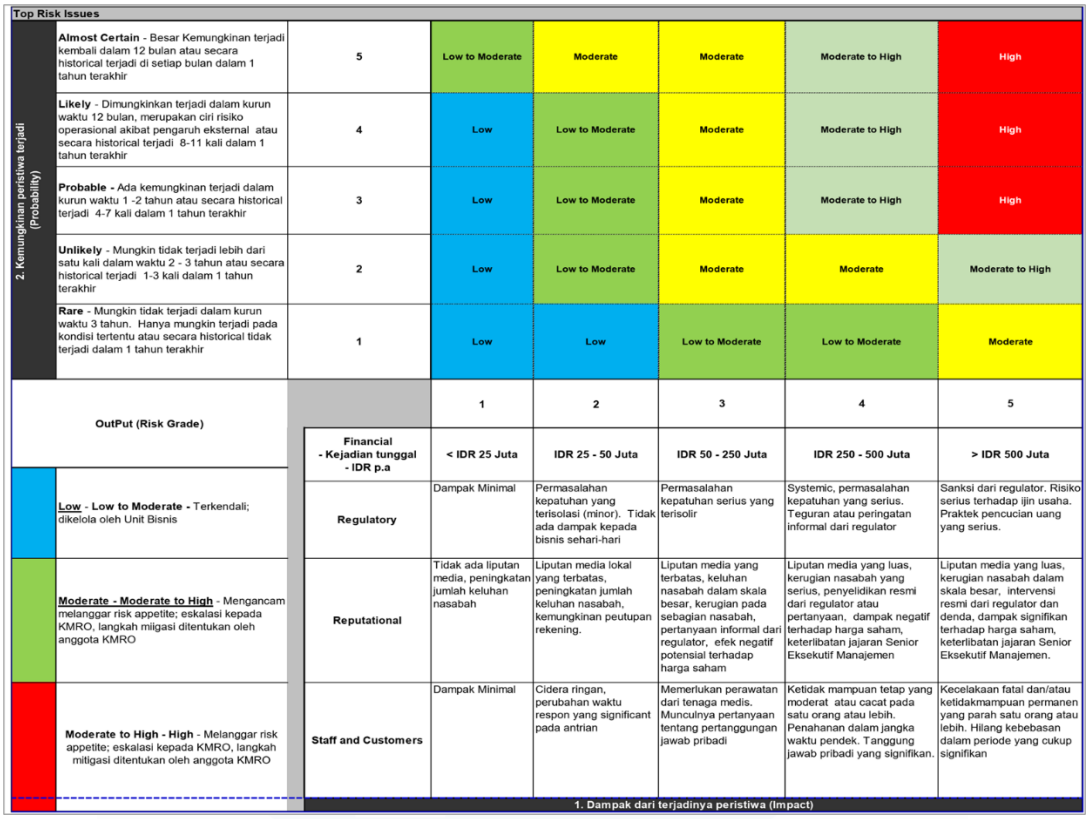
perlindungan data dan menjaga privasi data pribadi yang terdapat dalam perusahaan.

Untuk melaksanakan Data Protection Impact Assessment (DPIA), tim bekerja sama dengan vendor untuk menyusun panduan dan *template* seperti pada Gambar 3.20 yang akan membantu setiap unit kerja dalam melakukan analisis yang diperlukan. *Template* ini ditambahkan sebagai tab baru dalam file *template* yang digunakan untuk inventaris data pribadi yang telah selesai dilengkapi oleh masing-masing unit kerja. Tab tersebut digunakan untuk mengevaluasi potensi dampak dari setiap pemrosesan data pribadi yang dinilai memiliki risiko tinggi sesuai dengan Undang-undang Perlindungan Data Pribadi. Setiap pemrosesan data yang memiliki risiko tinggi akan memiliki tab Data Protection Impact Assessment (DPIA) tersendiri.



Gambar 3. 20 *Data Protection Impact Assessment (DPIA)* Bank Sahabat Sampoerna

Template tersebut mencakup deskripsi tentang risiko, probabilitas, dampak, tingkat risiko, mitigasi risiko, dampak mitigasi terhadap risiko, serta probabilitas dan dampak setelah mitigasi dilakukan. Penilaian probabilitas, dampak, dan tingkat risiko total mengacu pada konsep *Risk Grading Matrix* seperti yang ditunjukkan dalam Gambar 3.21.



Top Risk Issues

2. Kemungkinan peristiwa terjadi (Probability)							
	Almost Certain - Besar Kemungkinan terjadi kembali dalam 12 bulan atau secara historical terjadi di setiap bulan dalam 1 tahun terakhir	5	Low to Moderate	Moderate	Moderate	Moderate to High	High
	Likely - Dimungkinkan terjadi dalam kurun waktu 12 bulan, merupakan ciri risiko operasional akibat pengaruh eksternal atau secara historical terjadi 8-11 kali dalam 1 tahun terakhir	4	Low	Low to Moderate	Moderate	Moderate to High	High
	Probable - Ada kemungkinan terjadi dalam kurun waktu 1 -2 tahun atau secara historical terjadi 4-7 kali dalam 1 tahun terakhir	3	Low	Low to Moderate	Moderate	Moderate to High	High
	Unlikely - Mungkin tidak terjadi lebih dari satu kali dalam waktu 2 - 3 tahun atau secara historical terjadi 1-3 kali dalam 1 tahun terakhir	2	Low	Low to Moderate	Moderate	Moderate	Moderate to High
	Rare - Mungkin tidak terjadi dalam kurun waktu 3 tahun. Hanya mungkin terjadi pada kondisi tertentu atau secara historical tidak terjadi dalam 1 tahun terakhir	1	Low	Low	Low to Moderate	Low to Moderate	Moderate

OutPut (Risk Grade)		1	2	3	4	5
	Financial - Kejadian tunggal - IDR p.a	< IDR 25 Juta	IDR 25 - 50 Juta	IDR 50 - 250 Juta	IDR 250 - 500 Juta	> IDR 500 Juta
Low - Low to Moderate - Terkendali; dikelola oleh Unit Bisnis	**Regulatory**	Dampak Minimal	Permasalahan kepatuhan yang terisolasi (minor). Tidak ada dampak kepada bisnis sehari-hari	Permasalahan kepatuhan serius yang terisolir	Systemic, permasalahan kepatuhan yang serius. Teguran atau peringatan informal dari regulator	Sanksi dari regulator. Risiko serius terhadap ijin usaha. Praktek pencucian uang yang serius.
Moderate - Moderate to High - Mengancam melanggar risk appetite; eskalasi kepada KMRO, langkah mitigasi ditentukan oleh anggota KMRO	**Reputational**	Tidak ada liputan media, peningkatan jumlah keluhan nasabah	Liputan media lokal yang terbatas, peningkatan jumlah keluhan nasabah, kemungkinan peutupan rekening.	Liputan media yang terbatas, keluhan nasabah dalam skala besar, kerugian pada sebagian nasabah, pertanyaan informal dari regulator, efek negatif potensial terhadap harga saham	Liputan media yang luas, kerugian nasabah yang serius, penyelidikan resmi dari regulator atau pertanyaan, dampak negatif terhadap harga saham, keterlibatan jajaran Senior Eksekutif Manajemen	Liputan media yang luas, kerugian nasabah dalam skala besar, intervensi resmi dari regulator dan denda, dampak signifikan terhadap harga saham, keterlibatan jajaran Senior Eksekutif Manajemen.
Moderate to High - High - Melanggar risk appetite; eskalasi kepada KMRO, langkah mitigasi ditentukan oleh anggota KMRO	**Staff and Customers**	Dampak Minimal	Cidera ringan, perubahan waktu respon yang significant pada antrian	Memerlukan perawatan dari tenaga medis. Munculnya pertanyaan tentang pertanggungan jawab pribadi	Ketidak mampuan tetap yang moderat atau cacat pada satu orang atau lebih. Penahanan dalam jangka waktu pendek. Tanggung jawab pribadi yang signifikan.	Kecelakaan fatal dan/atau ketidakmampuan permanen yang parah satu orang atau lebih. Hilang kebebasan dalam periode yang cukup signifikan
		1. Dampak dari terjadinya peristiwa (Impact)				

Gambar 3. 21 *Risk Grading Matrix*

Setelah *template* disiapkan, tim memberikannya kepada masing-masing unit kerja untuk dilengkapi. Sebelum pengisian dilakukan, tim menyelenggarakan sesi diskusi pada setiap unit kerja, khususnya *Personal Data Protection (PDP)* Champion unit kerja tersebut, untuk memastikan pemahaman cara pengisian *template* tersebut. Selama proses pengisian, tim juga melakukan diskusi dengan setiap Personal Data Protection (PDP) Champion unit kerja dalam rangka menanggapi pertanyaan-pertanyaan terkait hal-hal maupun kekhawatiran yang berkaitan dengan pengisian Data Protection Impact Assessment (DPIA).

3.2.12 *Consent Management System*

Penulis bersama dengan tim internal Personal Data Protection bekerjasama dengan tim developer Bank Sahabat Sampoerna untuk mengembangkan *Consent Management System*. *Consent Management System* adalah sebuah sistem yang digunakan oleh Bank Sahabat Sampoerna untuk mengelola dan melacak persetujuan atau izin dari individu terkait penggunaan dan pemrosesan data pribadi

mereka. Sistem ini memungkinkan perusahaan untuk secara efisien mengelola persetujuan, termasuk mendokumentasikan, menyimpan, dan melacak status serta riwayat dari setiap persetujuan yang diberikan oleh nasabah. Selain itu, sistem ini juga membantu memudahkan pengguna untuk mengelola preferensi privasi dari nasabah, seperti penarikan kembali persetujuan oleh nasabah atau memperbarui preferensi privasi mereka. Dengan adanya *Consent Management System*, Bank Sahabat Sampoerna dapat memastikan bahwa perusahasan mematuhi peraturan perlindungan data dan memberikan nasabah kendali yang lebih besar atas data pribadi mereka.

Sebelum melanjutkan perancangan sistem lebih lanjut, tim mengumpulkan data pribadi pada setiap aplikasi yang terdampak. Tim meminta informasi mengenai setiap *field* data registrasi yang dikumpulkan oleh setiap aplikasi kepada penanggung jawab aplikasi. Setelah data terkumpul, penulis melakukan pemetaan setiap *field* tersebut dengan data Single CIF untuk menyusun *Consent Management System*.

Sebagai bagian dari proses perancangan sistem, penulis, yang merupakan mahasiswa magang di tim IT Business Enablement, bertanggung jawab untuk merancang antarmuka *Consent Management System*. Setelah melalui serangkaian *Focus Group Discussion (FGD)* bersama supervisor dan vendor, serta beberapa tahap revisi, rancangan antarmuka tersebut dapat dilanjutkan untuk nantinya sebagai acuan bagi tim *developer* dalam mengembangkan sistem. Sebelum merancang sistem, tim menyusun dokumen Architectural Decision Records (ADR) yang membantu dalam pengambilan keputusan arsitektural. Selain itu, penulis bersama dengan tim juga mengikuti IT Solution Advisory Board yang bertujuan memberikan panduan strategis, pengawasan, dan rekomendasi untuk memastikan sistem sesuai dengan tujuan perusahaan, mematuhi regulasi, dan diimplementasikan secara efektif. Dalam pengembangan desain UI sistem, penulis menggunakan *platform* Figma.

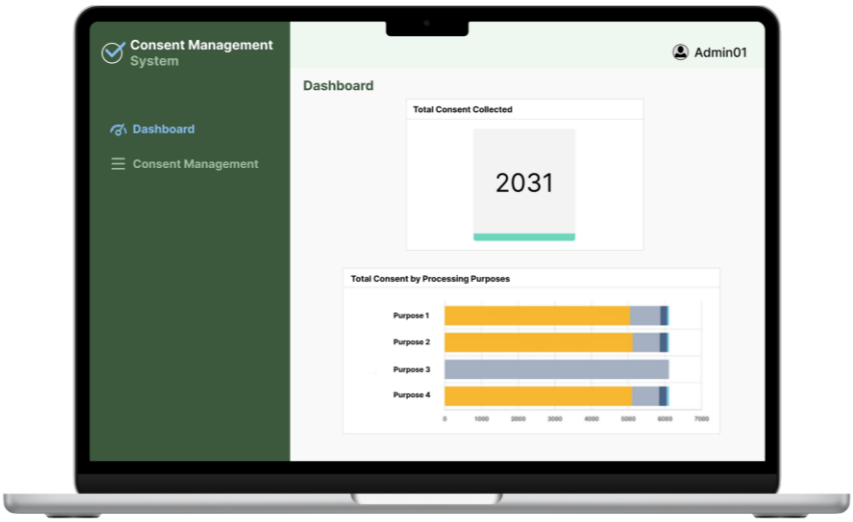
Gambar 3. 22 Logo Figma

Figma adalah sebuah *platform* desain berbasis web yang memungkinkan tim untuk berkolaborasi secara *real-time* dalam proses perancangan antarmuka pengguna tersebut. Dengan Figma, penulis dapat membuat *mockup* antarmuka yang interaktif dan mudah diakses oleh anggota tim lainnya. Hal ini penting karena tim *developer* perlu melakukan peninjauan dan memberikan komentar mengenai *mockup* yang dibuat oleh penulis. *Mockup* tersebut akan menjadi panduan bagi tim pengembang dalam proses pembuatan sistem, sehingga harus dipastikan bahwa desain UI yang dihasilkan sesuai dengan kebutuhan dan harapan semua pihak yang terlibat. *Platform* ini menyediakan berbagai fitur yang memungkinkan penulis untuk membuat desain yang responsif dan estetis, seperti kemampuan untuk membuat prototipe interaktif, berbagi komponen yang dapat digunakan ulang, serta memberikan komentar dan umpan balik secara langsung pada desain. Dengan menggunakan Figma, penulis dapat memastikan bahwa desain UI untuk *Consent Management System* sesuai dengan kebutuhan dan standar perusahaan, serta memudahkan tim untuk berkolaborasi dalam proses pengembangan sistem secara efisien.

Setelah sistem terbentuk, serah terima dilakukan kepada Data Protection Officer (DPrO), sebuah posisi baru di Bank Sahabat Sampoerna yang dibentuk karena kebijakan regulasi yang baru. DPrO sendiri memiliki tanggung jawab dalam mengawasi dan mengelola kebijakan, prosedur, dan praktik perlindungan data pribadi dalam perusahaan. Dalam mengelola sistem, DPrO akan dibantu oleh Data

Steward yang secara spesifik lebih berfokus pada manajemen operasional dan teknis dari data dalam perusahaan, termasuk pemeliharaan kualitas data, pengelolaan metadata, dan pemahaman yang mendalam tentang data yang digunakan dan disimpan dalam sistem. Berikut adalah tampilan antarmuka *Consent Management System* yang telah dirancang oleh penulis.

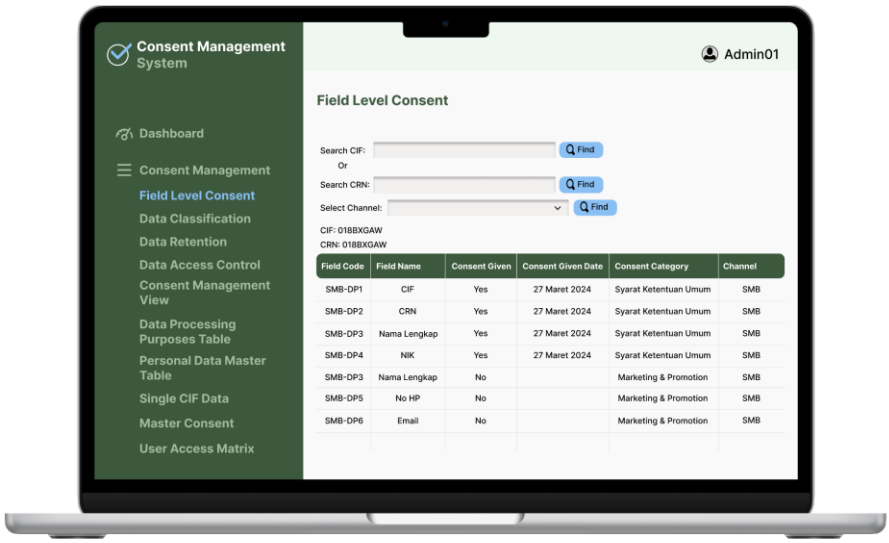
Ketika pengguna masuk ke dalam sistem, pengguna akan diarahkan ke halaman *dashboard* seperti pada Gambar 3.23. Di sini, pengguna akan melihat visualisasi statistik mengenai jumlah total *consent flag* yang ada dalam sistem, serta jumlah *consent* yang diberikan oleh nasabah berdasarkan tujuan pemrosesan data, seperti untuk keperluan pemasaran, analisis perusahaan, dan lain sebagainya. Pada menu Consent Management, terdapat 10 submenu yang masing-masing memiliki fungsi berbeda dalam pengelolaan *consent* untuk data pribadi yang disimpan di Bank Sahabat Sampoerna.



Gambar 3. 23 Halaman *Dashboard*

Submenu Field Level Consent seperti pada Gambar 3.24 merupakan bagian dari fungsi pengelolaan *consent* yang memungkinkan pengguna untuk memantau dan mengelola persetujuan akses data pada tingkat *field* atau kolom tertentu yang

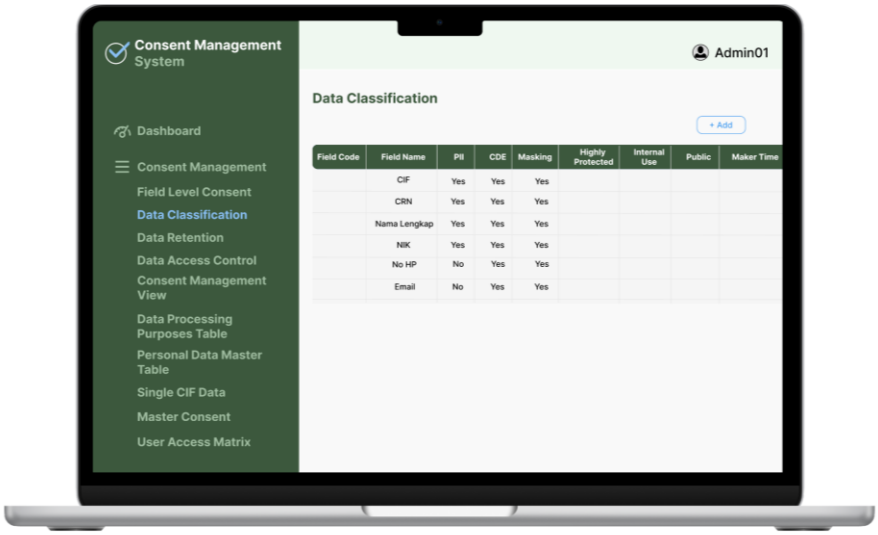
diberikan dari nasabah kepada perusahaan, seperti nama lengkap, nomor telepon, email, dan Nomor Induk Kependudukan (NIK). Pada submenu ini, pengguna dapat melihat daftar *consent* tersebut pada tingkat *field* secara terperinci, mulai dari kode *field* terkait, tanggal *consent* tersebut diberikan, hingga kategori *consent* dan *channel*-nya. Pengguna juga dapat melakukan pencarian berdasarkan nomor Customer Information File (CIF) atau Customer Reference Number (CRN) beserta *channel* atau aplikasi di mana nasabah tersebut memberikan *consent*.



Gambar 3. 24 Sub Menu *Field Level Consent*

Pada submenu Data Classification seperti yang ditunjukkan pada Gambar 3.25, pengguna dapat melihat klasifikasi data yang lebih rinci terkait setiap field atau kolom dalam basis data. Klasifikasi ini mencakup informasi apakah suatu *field* data termasuk dalam kategori *Personally Identifiable Information* (PII), *Critical Data Elements* (CDE), apakah data tersebut di-*masking*, dan berbagai klasifikasi lainnya. *Personally Identifiable Information* (PII) merujuk kepada jenis data yang dapat digunakan secara langsung atau tidak langsung untuk mengidentifikasi individu tertentu, seperti nama, alamat, atau nomor identifikasi. Sementara itu, *Critical Data Elements* (CDE) adalah data yang dianggap penting atau kritis dalam

konteks operasional perusahaan. Dengan informasi klasifikasi ini, pengguna dapat dengan mudah mengidentifikasi jenis data *field* terkait, apakah data tersebut termasuk dalam kategori yang sensitif atau tidak, dan apakah data tersebut di-*masking* untuk keperluan keamanan. Bagian ini juga diperlukan untuk pengelolaan data yang tepat dan sesuai dengan kebijakan perlindungan data. Pada submenu ini, terdapat *button* Add yang dapat digunakan untuk menambahkan klasifikasi data yang baru.



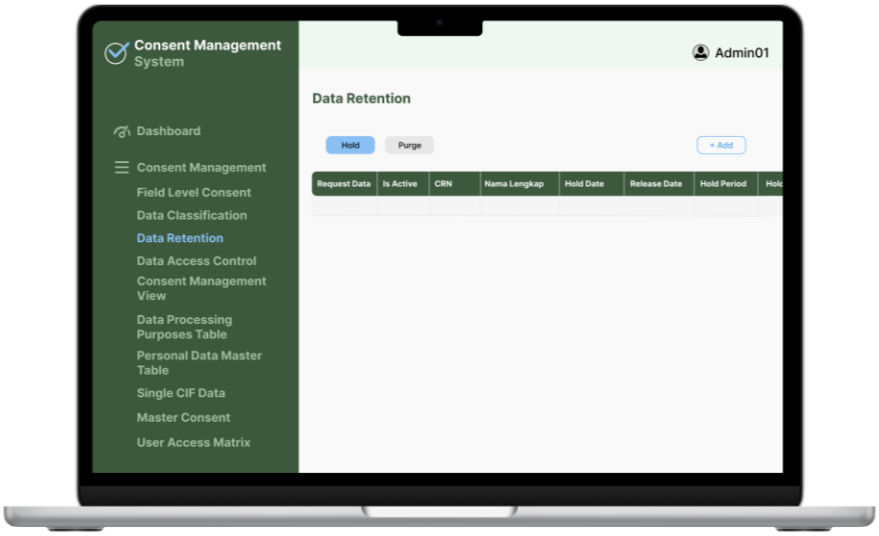
Gambar 3. 25 *Data Classification*

Submenu Data Retention seperti yang ditunjukkan pada Gambar 3.26 merupakan halaman untuk mengatur berapa lama perusahaan akan menyimpan atau memelihara data tertentu sebelum data tersebut dihapus atau dihancurkan. Kebijakan retensi data ini melibatkan menetapkan rentang waktu tertentu selama data harus tetap tersedia untuk keperluan operasional, kepatuhan hukum, atau kebutuhan bisnis.

Pada submenu ini, terdapat dua *tab,* yaitu Hold dan Purge. *Hold* merupakan tindakan yang diambil untuk menunda atau mempertahankan data dari proses penghapusan, penggunaan data, atau proses lain. Pada *tab* ini, pengguna dapat

menambahkan data yang ingin di-*hold.* Setelah ditambahkan, data tersebut akan tercantum dalam tabel yang telah tersedia.

Purge adalah tindakan yang diambil untuk menghilangkan atau memusnahkan data. Selama proses penghapusan data, sistem akan mempertimbangkan dan menganalisis data dengan pemeriksaan ketergantungan apakah nasabah masih memiliki *flag* aktif atau tidak.

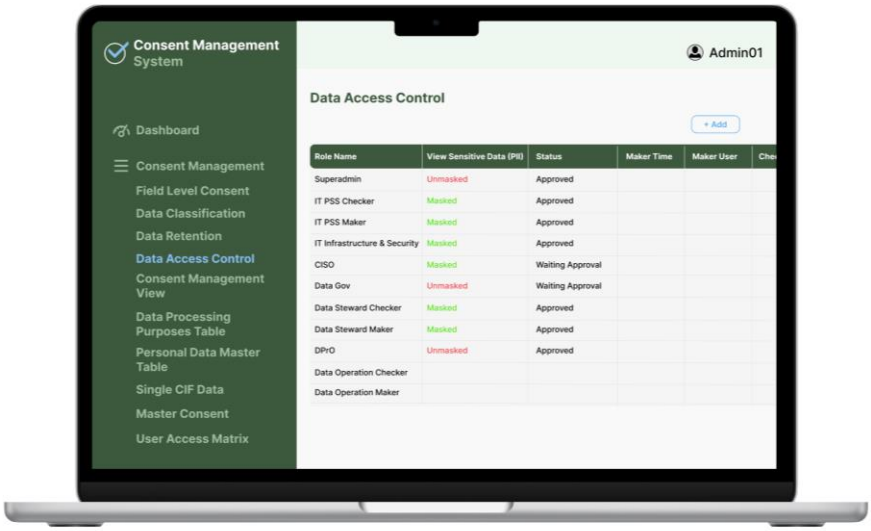


Gambar 3. 26 Sub Menu *Data Retention*

Kontrol akses data merujuk pada serangkaian praktik, kebijakan, dan langkah-langkah yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data. Implementasi submenu Data Access Control seperti pada Gambar 3.27 membantu menciptakan lapisan keamanan yang kokoh untuk melindungi data dari ancaman keamanan dan memastikan bahwa hanya pihak yang diotorisasi yang dapat mengakses dan memanfaatkannya sesuai dengan kebijakan yang telah ditetapkan.

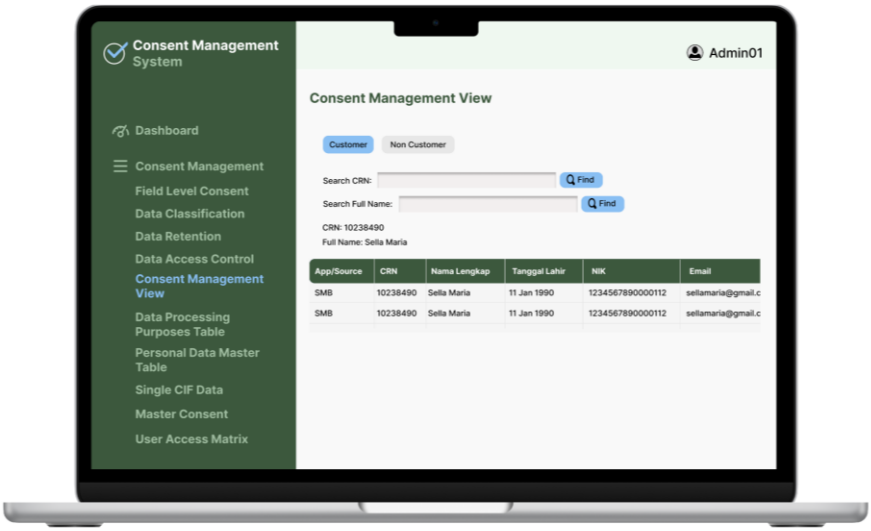
Pada submenu ini, pengguna dapat melihat daftar posisi karyawan perusahaan yang dapat mengakses data-data sensitif, yaitu Personal Identifiable Information (PII), jenis *masking* untuk setiap posisi tersebut (apakah di-*mask* atau tidak), serta informasi rinci mengenai akses kontrol data tersebut dalam sebuah

tabel. Tidak hanya melihat, pengguna juga dapat menambahkan baris data yang baru. Kontrol akses data yang baru ditambahkan tersebut harus mendapatkan persetujuan atau perizinan dari penanggung jawab *Consent Management System* dan Personal Data Protection tertinggi di perusahaan.



Gambar 3. 27 Sub Menu *Data Access Control*

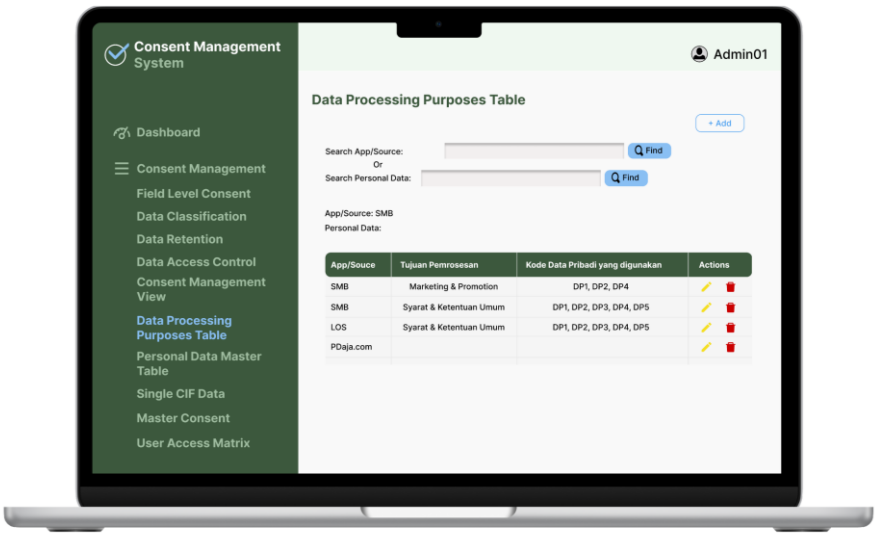
Submenu Consent Management View seperti yang ditunjukkan pada Gambar 3.28 merupakan bagian dari sistem yang memungkinkan pengguna untuk melihat tabel data pribadi nasabah berdasarkan aplikasi dan Customer Reference Number (CRN). Di halaman ini, pengguna dapat melakukan pencarian data dengan memasukkan Customer Reference Number (CRN) dan nama lengkap nasabah untuk menemukan informasi yang dibutuhkan. Tampilan tabel menyediakan rincian data mengenai data pribadi nasabah yang telah disimpan dalam sistem. Hal ini memudahkan pengguna dalam mengelola dan mengakses informasi yang relevan sesuai kebutuhan mereka.



Gambar 3. 28 Sub Menu *Consent Management View*

Submenu Data Processing Purposes Table seperti yang ditunjukkan pada Gambar 3.29 merupakan fitur yang memungkinkan pengguna untuk mengelola tujuan pemrosesan data berdasarkan tingkat abstraksi tujuan. Pada halaman ini, pengguna dapat melihat tabel yang mencantumkan informasi mengenai aplikasi atau sumber data, tujuan pemrosesan data, dan kode data pribadi yang terkait. Di sini, pengguna dapat melakukan pencarian dengan memasukkan nama aplikasi atau sumber data atau dengan mencari data pribadi yang relevan. Selain itu, fitur ini juga memungkinkan pengguna untuk menambahkan entri baru ke dalam tabel untuk mencatat tujuan pemrosesan data baru yang ingin ditambahkan ke dalam sistem.

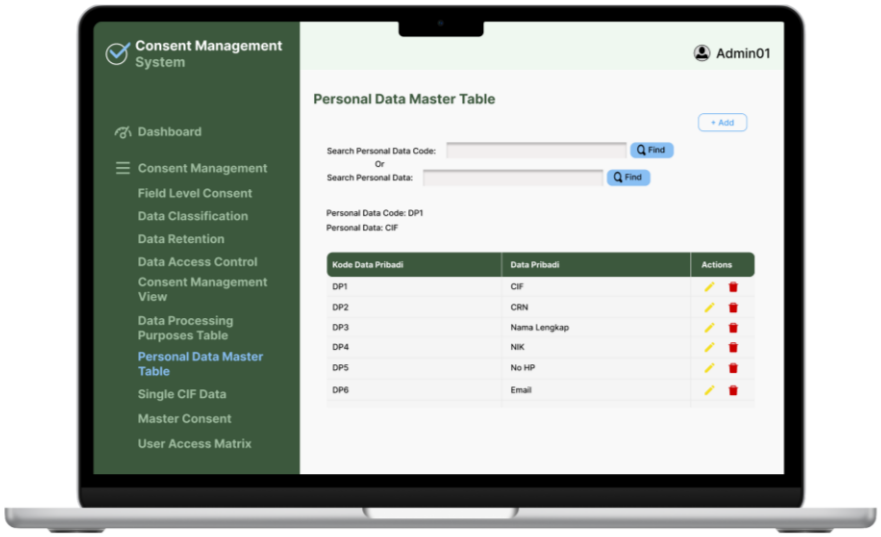
Dengan menggunakan submenu Data Processing Purposes Table, pengguna memiliki kendali lebih dalam mengatur penggunaan data mereka. Mereka dapat memilih dan menyesuaikan data pribadi yang dibutuhkan menyesuaikan dengan tujuan pemrosesan data sesuai kebutuhan dan preferensi mereka.



Gambar 3. 29 Sub Menu *Data Processing Purposes Table*

Submenu Personal Data Master Table seperti yang ditunjukkan pada Gambar 3.30 merupakan fitur yang memuat tabel data master yang mencantumkan kode data pribadi beserta dengan deskripsi data pribadi yang sesuai. Pengguna dapat dengan mudah mengacu atau mereferensi dari tabel ini untuk melihat deskripsi dari kode data pribadi tertentu. Pengguna dapat dengan mudah mencari informasi dalam tabel ini dengan memasukkan kode data pribadi atau deskripsi data pribadi yang ingin dicari. Selain itu, terdapat juga *button* Add yang memungkinkan pengguna untuk menambahkan entri baru ke dalam tabel untuk memperbarui atau melengkapi data pribadi tersebut.

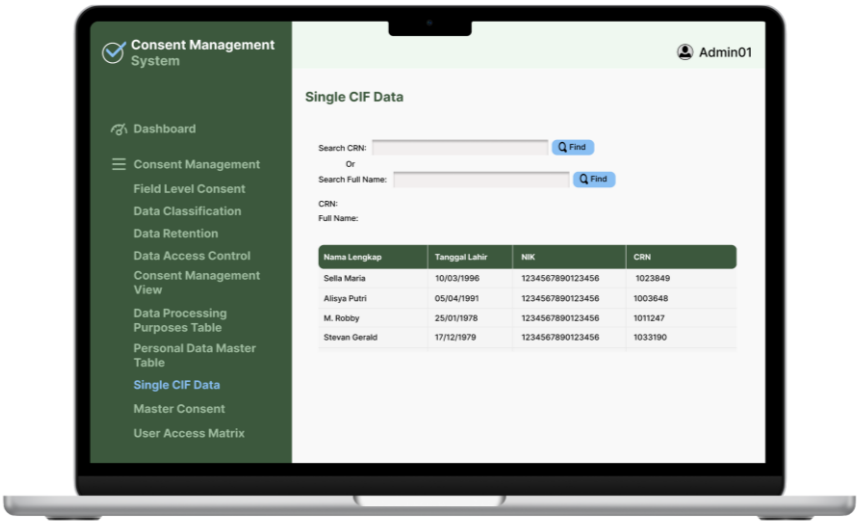
Submenu ini membantu perusahaan dalam mengelola data pribadi secara efisien dan akurat. Dengan adanya tabel data master, pengguna dapat dengan cepat mengidentifikasi dan melacak kode-kode dari berbagai jenis data pribadi yang tersedia dalam sistem.



Gambar 3. 30 Sub Menu *Personal Data Master Table*

Submenu Single CIF Data seperti yang ditunjukkan pada Gambar 3.31 merupakan fitur yang menyajikan tabel data tunggal yang mencakup informasi penting mengenai nasabah. Dalam tabel ini, pengguna dapat menemukan data seperti nama lengkap, tanggal lahir, Nomor Induk Kependudukan (NIK), dan Customer Reference Number (CRN). Dengan adanya fitur pencarian pada submenu ini, pengguna dapat dengan mudah mencari data berdasarkan kode unik setiap nasabah atau nama lengkap nasabah tanpa harus melalui proses manual yang memakan waktu.

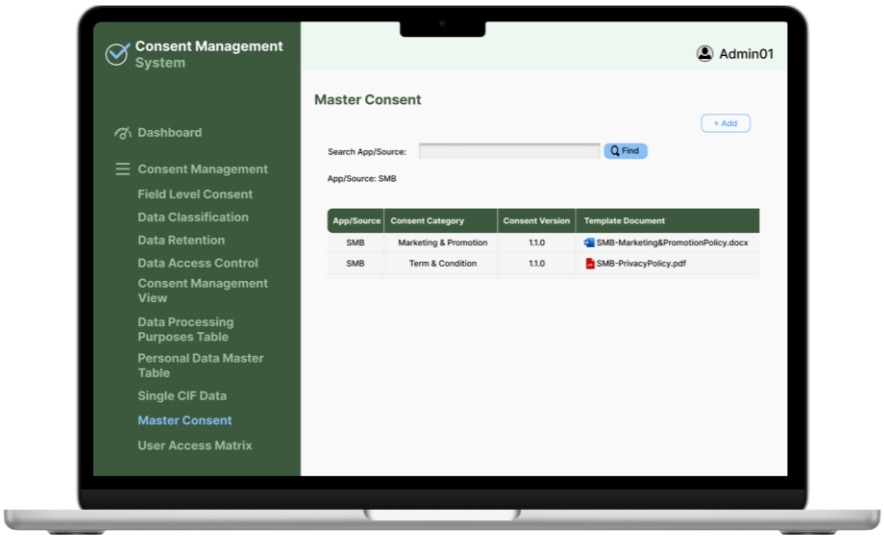
Hal ini memungkinkan pengguna untuk dengan cepat menemukan informasi yang mereka butuhkan dan melakukan pemrosesan data maupun memberikan pelayanan kepada nasabah dengan lebih efisien.



Gambar 3. 31 Sub Menu *Single CIF Data*

Submenu Master Consent yang ditunjukkan pada Gambar 3.32 menyimpan informasi penting mengenai *template* dari setiap dokumen permintaan *consent* kepada nasabah dari setiap aplikasi. Selain dokumen *template*, submenu ini juga menyimpan secara rinci informasi tentang *template* tersebut seperti aplikasi sumbernya, jenis atau kategori *consent* yang diminta, serta versi *consent* tersebut.

Submenu ini juga memungkinkan pengguna untuk melakukan pencarian entri atau data berdasarkan aplikasi sumbernya. Di sini, pengguna juga dapat menambahkan entri baru untuk memasukkan dokumen template yang baru, seperti saat permintaan *consent* baru diajukan atau ada pembentukan aplikasi baru yang memerlukan template dokumen khususnya sendiri.



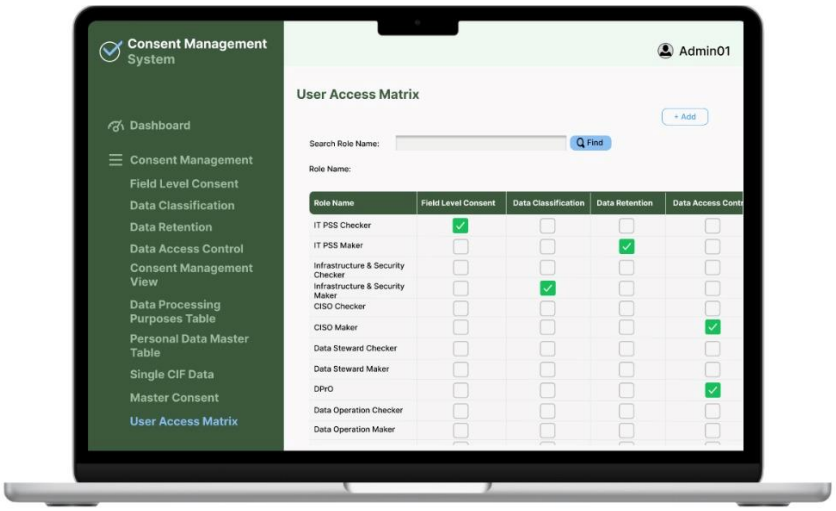
Gambar 3. 32 Sub Menu *Master Consent*

Submenu User Access Matrix seperti yang ditunjukkan pada Gambar 3.33 adalah bagian dari *Consent Management System* yang dirancang untuk mengelola hak akses pengguna berdasarkan peran atau *role* dalam perusahaan. Tampilan utamanya adalah dalam bentuk tabel yang mencantumkan nama setiap *role* dalam perusahaan. Setiap kolom tabel menampilkan submenu dari *Consent Management System* yang perlu diberikan hak akses, di mana *value* dari setiap kolom tersebut merupakan *checkbox* untuk memberikan jenis akses kepada setiap *role*.

Ada dua jenis akses yang dapat diberikan, yaitu:

- *Checker:* Merupakan *role* yang bertanggung jawab untuk melakukan pengecekan dan memberikan persetujuan atau penolakan terhadap permintaan yang masuk. Mereka memiliki hak akses untuk melihat, menyetujui, atau menolak permintaan, tetapi tidak dapat melakukan perubahan pada data.
- *Maker:* Merupakan *role* yang memiliki hak akses lebih lanjut, termasuk kemampuan untuk mengedit dan menghapus data. Mereka dapat membuat permintaan baru, melakukan perubahan pada data, serta menghapus entri.

Fitur lain pada submenu User Access Matrix adalah kemampuan untuk melakukan pencarian berdasarkan nama peran (*role name*), yang memudahkan pengguna dalam menemukan dan mengelola hak akses. Selain itu, pengguna juga dapat menambahkan *role* baru beserta hak aksesnya dengan mudah melalui *button* Add, yang memperluas fleksibilitas dalam mengelola struktur perusahaan dan hak akses dalam *Consent Management System*.



Gambar 3. 33 Sub Menu *User Access Matrix*

3.2.13 Enhancement 10 Aplikasi Customer Facing

Untuk meningkatkan fungsi setiap aplikasi terkait Perlindungan Data Pribadi, tim berkolaborasi dengan Senior Management Team (SMT) yang bertanggung jawab atas masing-masing aplikasi tersebut. Sebagai langkah awal, tim melakukan uji coba dengan sepuluh aplikasi yang paling umum digunakan oleh nasabah sebagai aplikasi *pilot*.

Setelah mempelajari dan mengevaluasi kesepuluh aplikasi *pilot* tersebut, tim mengadakan rapat diskusi dengan setiap Senior Management Team (SMT) dan anggota tim mereka. Kesepuluh aplikasi ini secara keseluruhan dikelola oleh tiga Senior Management Team (SMT) yang berasal dari divisi IT Business Enablement,

yaitu unit kerja *Core & General Services, Bank as a Service (BaaS),* dan *Delivery Channel*. Diskusi ini bertujuan untuk memastikan bahwa tim pemegang aplikasi memahami perubahan yang harus mereka lakukan, seperti penambahan *flag* baru, pengaruhnya terhadap *database*, kemungkinan penambahan klausal pada syarat dan ketentuan, dan sebagainya.

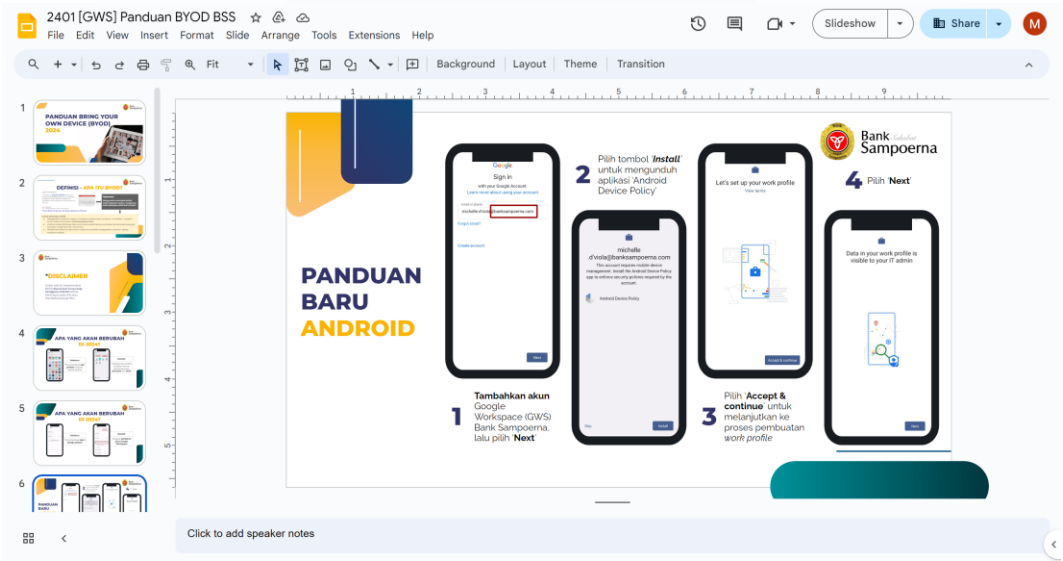
Untuk memfasilitasi proses pengembangan pada setiap aplikasi, tim menyusun Business Requirenment Documents (BRD) seperti yang ditunjukkan pada Gambar 3.34. Setelah Business Requirenment Documents (BRD), selesai disusun, dokumen tersebut akan diserahkan kepada pemegang aplikasi sebagai acuan untuk memulai pelaksanaan proyek ini.

Gambar 3. 34 *Business Requirenment Documents (BRD) Enhancement* 10 Aplikasi

3.2.14 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) merupakan proyek tambahan yang ditugaskan kepada penulis oleh Direktur Information Technology. Tugas penulis dalam proyek ini adalah menyusun materi panduan untuk memperkenalkan konsep Bring Your Own Device (BYOD) kepada karyawan perusahaan. Materi yang disusun oleh penulis ini bertujuan untuk menjelaskan kepada karyawan tentang konsep Bring Your Own Device (BYOD), perbedaan yang akan terjadi setelah penerapan Bring Your Own Device (BYOD), dan memberikan panduan migrasi serta penggunaannya. Penerapan Bring Your Own Device (BYOD) ini akan melibatkan migrasi dari *platform* yang sebelumnya digunakan ke *platform* yang

disediakan oleh perusahaan. Salah satu cuplikan dari materi yang disiapkan oleh penulis dapat dilihat dalam Gambar 3.35 berikut.



Gambar 3. 35 Materi *Bring Your Own Device (BYOD)*

Perubahan yang akan terjadi termasuk kemampuan karyawan untuk menggunakan laptop pribadi mereka untuk pekerjaan, yang sebelumnya hanya menggunakan laptop kantor. Untuk menambahkan akun atau *email* kantor di *smartphone*, karyawan perlu menginstal Android Device Policy, yang akan memastikan keamanan data perusahaan dengan mencegah fungsi seperti *screenshot* saat dalam mode kerja. Dengan demikian, Bring Your Own Device (BYOD) memberikan fleksibilitas bagi karyawan untuk menggunakan perangkat pribadi mereka sambil tetap menjaga keamanan data perusahaan.

Gambar 3. 36 Logo Google Workspace

Bring Your Own Device (BYOD) pada Bank Sahabat Sampoerna akan memanfaatkan Google Workspace untuk berbagai keperluan, seperti penggantian penggunaan WhatsApp dengan Google Chat untuk komunikasi bisnis dan penggantian penggunaan Outlook dengan Gmail. Adapun Google Workspace memiliki definisi sebagai kumpulan produktivitas berbasis *cloud* yang mencakup berbagai aplikasi seperti Gmail, Google Drive, Google Docs, Google Sheets, Google Slides, Google Meet dan masih banyak lagi. *Platform* ini digunakan untuk membantu individu dan tim bekerja secara kolaboratif. Google Workspace memungkinkan pengguna untuk berbagi dan mengedit dokumen secara *real-time*, mengelola kalender, mengirim *email*, serta melakukan *meeting* virtual. Dengan akses yang mudah dari berbagai perangkat, Google Workspace dapat memfasilitasi kerja tim yang efisien, fleksibel, dan terintegrasi. Hal ini mempercepat proses kerja dan meningkatkan produktivitas secara keseluruhan dalam perusahaan.

Penulis secara berkala melakukan diskusi dengan Direktur Information Technology dan berkolaborasi dengan unit kerja IT Infrastructure & Security Development, yang bertanggung jawab atas proyek Bring Your Own Device (BYOD) dan penyampaian materi sosialisasinya. Materi yang disusun oleh penulis bertujuan untuk membantu karyawan dalam menambahkan akun Google Workspace (GWS) Bank Sampoerna ke perangkat mereka masing-masing.

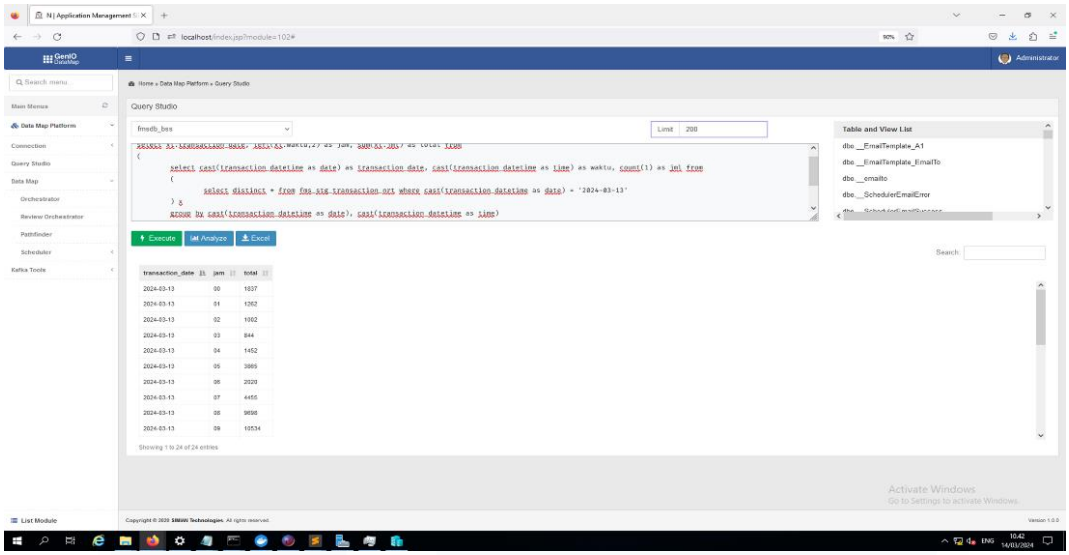
3.2.15 Visualisasi Fraud Management System

Fraud Management System merupakan suatu proyek tambahan dimana penulis ditempatkan oleh supervisor. Supervisor penulis juga menjabat sebagai Project Manager dari proyek Fraud Management System, sebagaimana beliau adalah Project Manager dari proyek Personal Data Protection.

Peran penulis dalam proyek Fraud Management System adalah memantau data transaksi harian. Proses pengambilan data dilakukan melalui *query* menggunakan bahasa SQL.

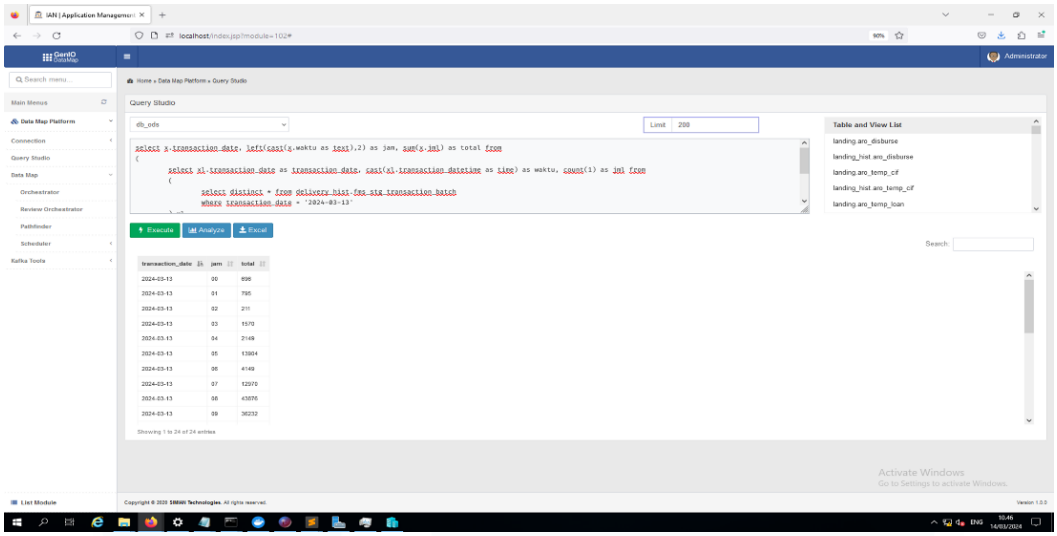
Gambar 3. 37 Logo SQL

Dalam sistem Fraud Management System, terdapat dua jenis data transaksi dalam *database*, yaitu Near Real Time (NRT) dan Batch. Transaksi Near Real Time (NRT) mengacu pada transaksi yang diproses secara langsung saat terjadi. Contoh transaksi ini meliputi transfer antar rekening bank, penarikan uang tunai dari ATM, pembayaran menggunakan kartu debit atau kredit, serta pengecekan saldo rekening secara langsung. Adapun *query* yang dituliskan untuk melakukan penarikan data NRT adalah seperti pada Gambar 3.38 berikut.



Gambar 3. 38 Query Penarikan *Data Near Real Time (NRT)*

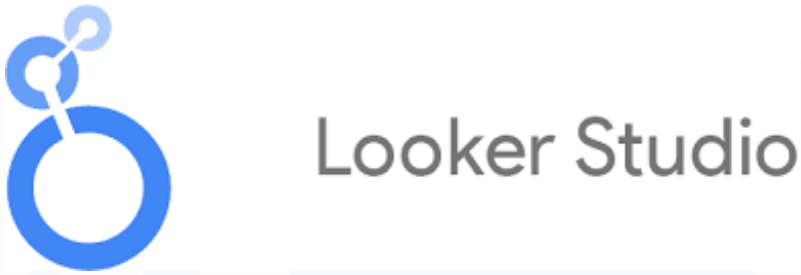
Transaksi Batch melibatkan pengumpulan transaksi dalam kelompok untuk diproses bersamaan pada waktu tertentu, seperti pada akhir hari kerja. Dalam sistem Fraud Management System, proses penyelesaian *job* data dilakukan pada hari berikutnya. Oleh karena itu, untuk mendapatkan keseluruhan data transaksi dari hari sebelumnya, proses pengambilan data dilakukan pada pagi hari sekitar jam 10 hingga 11. Proses *batch* ini umumnya digunakan untuk transaksi yang tidak memerlukan pemrosesan instan dan respons cepat. Sebagai contoh, transaksi kartu kredit pada akhir hari kerja sering kali dimasukkan dalam kategori transaksi *batch*. Adapun *query* yang dituliskan untuk melakukan penarikan data *batch* adalah seperti pada Gambar 3.39 berikut.



Gambar 3. 39 Query Penarikan *Batch*

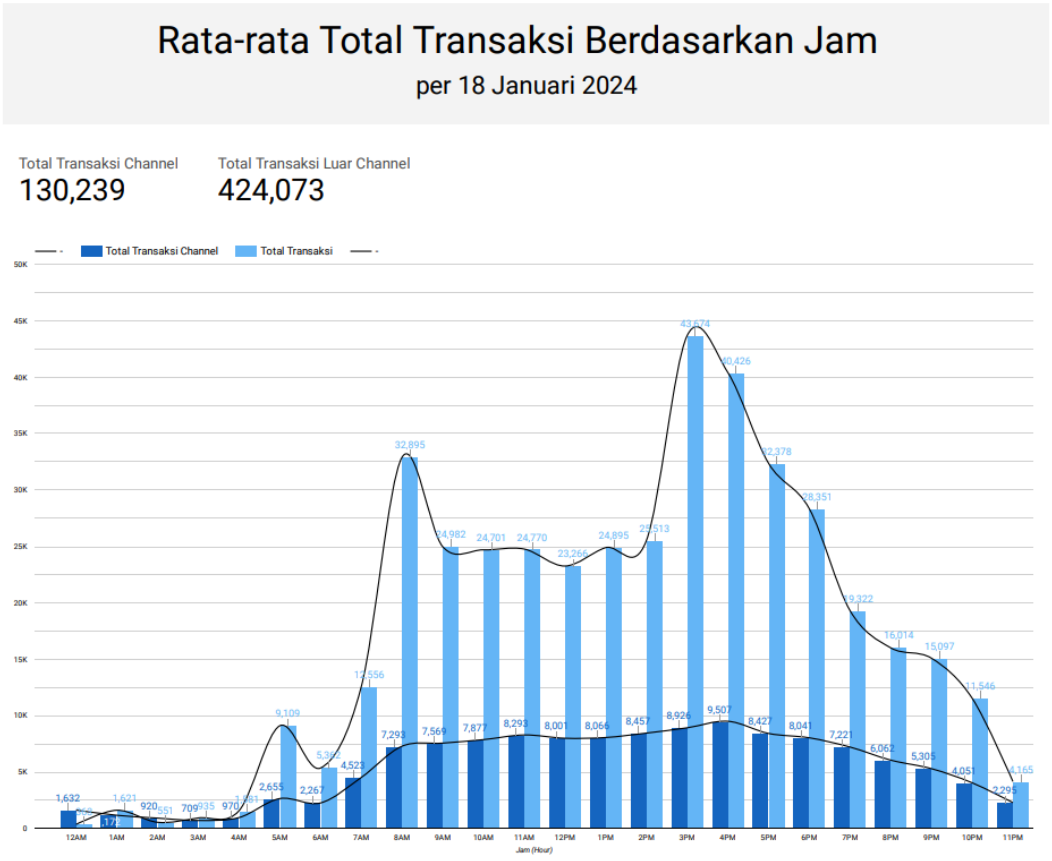
Setelah menulis *query* pada *database*, data diekstrak ke dalam format Microsoft Excel. File Microsoft Excel tersebut kemudian dipindahkan ke Google Sheets untuk kemudahan pengolahan, karena akan digunakan untuk membuat visualisasi menggunakan Google Looker Studio. Seluruh visualisasi yang dibuat oleh penulis digunakan dalam rapat untuk memantau kinerja sistem yang baru diimplementasikan ini.

Google Looker Studio merupakan *platform* analitik yang disediakan oleh Google dan memungkinkan pengguna untuk dengan mudah menjelajahi, menganalisis, dan memvisualisasikan data secara mendalam. Dengan antarmuka yang intuitif dan berbasis *web*, Looker Studio memungkinkan pengguna dari berbagai tingkatan keahlian untuk membuat dan menyesuaikan visualisasi maupun *dashboard* data tanpa perlu pengetahuan teknis yang mendalam. Hal ini membantu pengguna untuk menggali wawasan yang berharga dari data bisnis dengan cepat dan efisien untuk mendukung pengambilan keputusan yang lebih baik dan respons yang lebih cepat terhadap perubahan pasar. Namun, meskipun dirancang untuk kemudahan penggunaan, kekurangannya terletak pada keterbatasan fitur jika dibandingkan dengan *platform* analitik seperti Tableau atau Power BI.



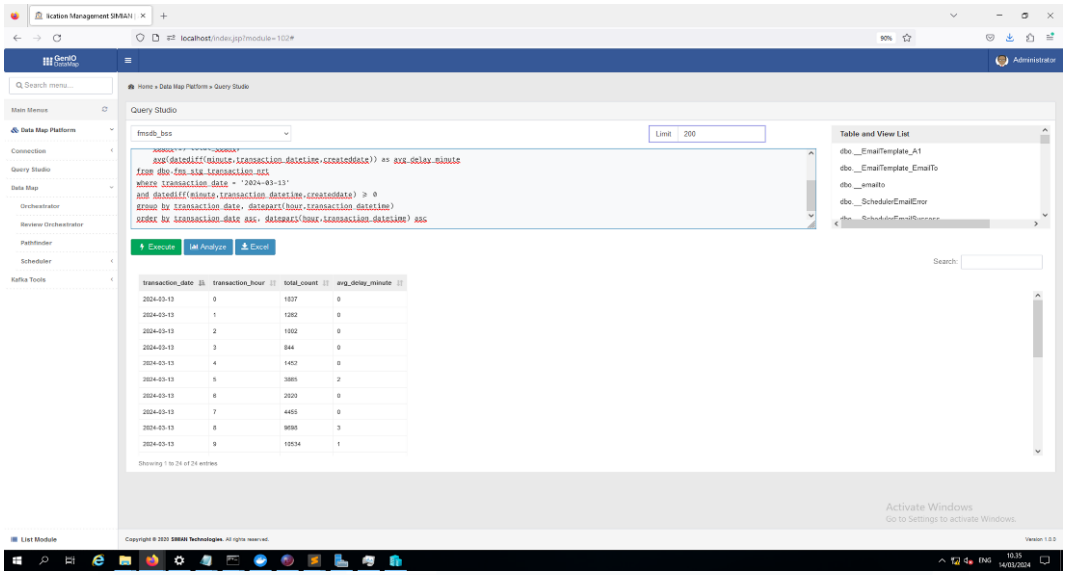
Gambar 3. 40 Logo Looker Studio

Dashboard yang dibuat oleh penulis menampilkan hasil tarikan data harian dalam bentuk visualisasi seperti yang terlihat pada Gambar 3.41 berikut. Pada *dashboard* tersebut, terdapat visualisi berupa *card* untuk menampilkan jumlah total rata-rata transaksi per jam untuk dua jenis transaksi, yaitu transaksi channel (NRT) dan transaksi di luar channel (Batch) pada hari tersebut. Selain itu, *dashboard* juga memuat visualisasi grafik menggunakan *barchart* dan *linechart*. *Barchart* digunakan untuk menampilkan jumlah rata-rata transaksi secara tepat per jam, sementara *linechart* digunakan sebagai alternatif *trendline* karena keterbatasan fitur dari Looker Studio ini.



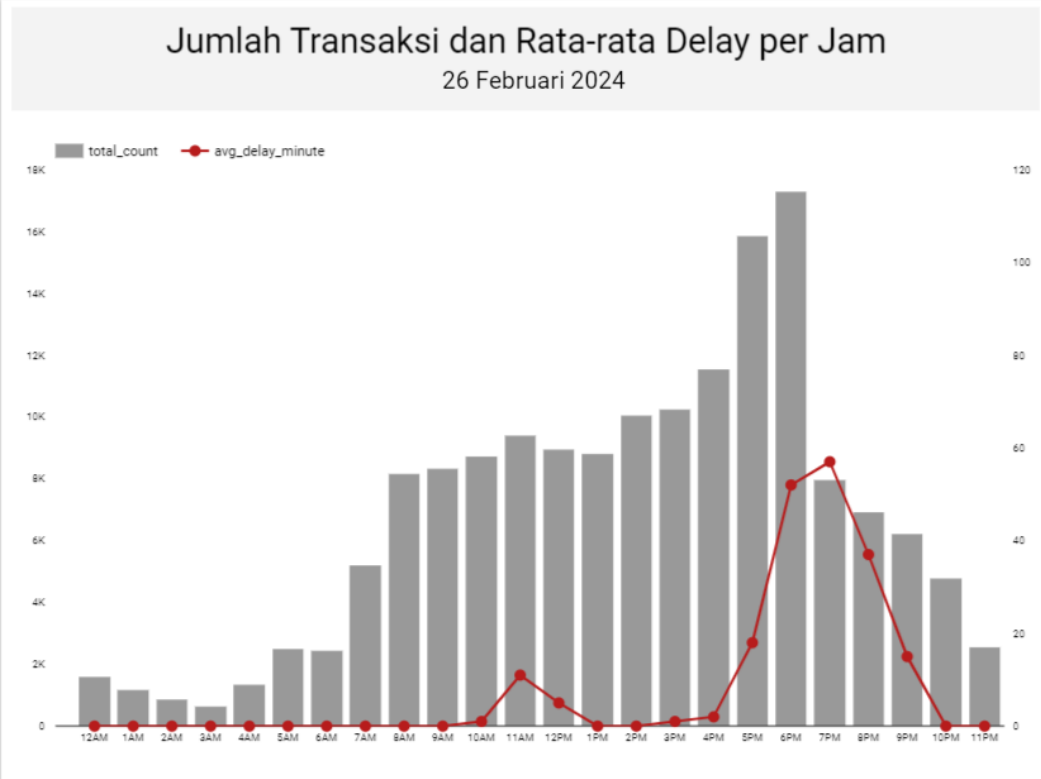
Gambar 3. 41 Visualisasi Data Rata-rata Total Transaksi Berdasarkan Jam

Selain digunakan untuk memantau jumlah transaksi harian, penulis juga melakukan penarikan data dari *database* ke dalam format Microsoft Excel untuk memantau keterlambatan atau *delay* pada sistem yang seharusnya tidak terjadi. Adapun *query* penarikan data yang dituliskan adalah seperti pada Gambar 3.42 berikut.



Gambar 3. 42 Query *Monitoring* Data Transaksi

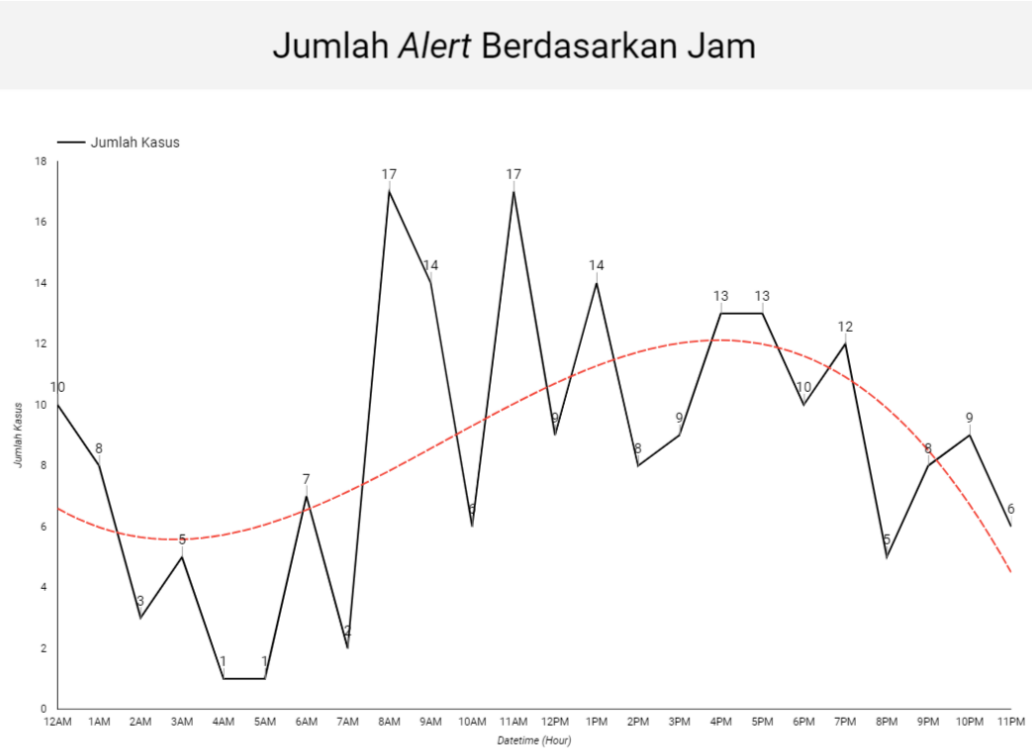
Seperti sebelumnya, data ini juga dipindahkan ke Google Sheet agar lebih mudah divisualisasikan menggunakan Google Looker Studio. Hasil visualisasi ini berguna bagi tim Fraud Management System dalam menganalisis penyebab *delay* pada sistem, merencanakan solusi, serta memantau kemajuan setelah masalah tersebut diatasi. Seperti sebelumnya, proses pembuatan visualisasi keterlambatan ini juga dilakukan setiap harinya. Visualisasi data tersebut adalah seperti pada Gambar 3.43 berikut.



Gambar 3. 43 Visualisasi Data Jumlah Transaksi dan Rata-rata *Delay* per Jam

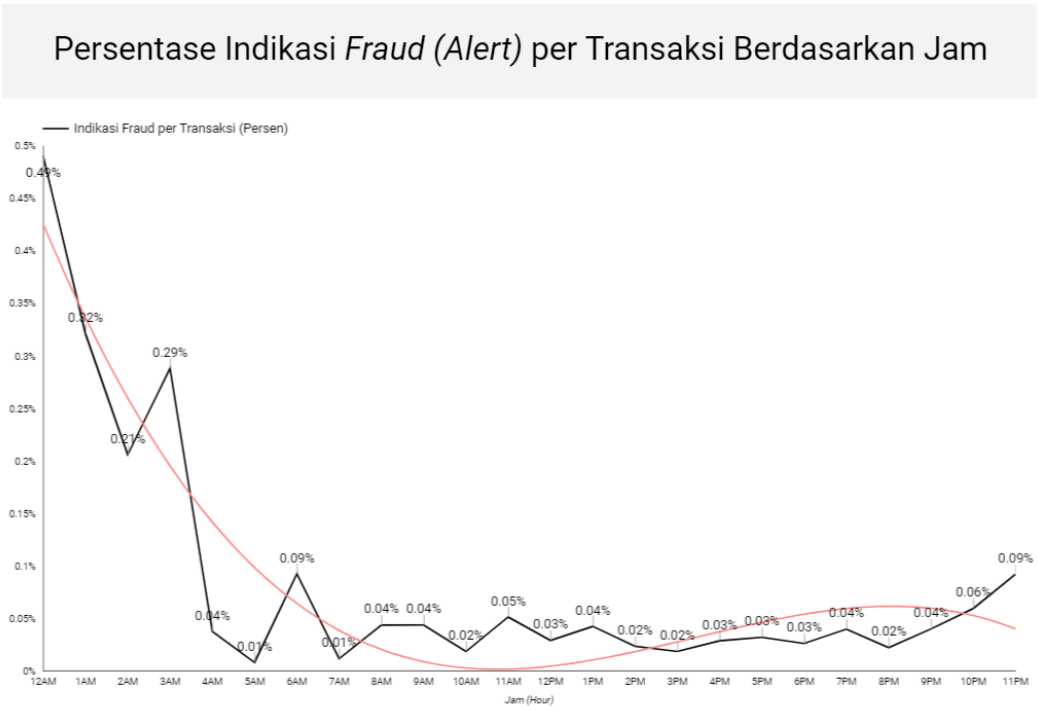
Visualisasi *delay* dibuat menggunakan dual *axis*, yaitu terdiri dari *barchart* dan *linechart*. *Barchart* digunakan untuk menggambarkan tren jumlah rata-rata transaksi per jam, sementara *linechart* dengan warna merah menunjukkan rata-rata keterlambatan dari setiap transaksi per jam, diukur dalam satuan menit.

Penulis juga bertanggung jawab untuk membuat visualisasi jumlah *alert* berdasarkan jam seperti pada Gambar 3.44. Hal ini bertujuan untuk membantu pemantauan pada jam-jam tertentu di mana indikasi *fraud* paling sering terjadi, sehingga dapat mendukung perencanaan keamanan sistem secara lebih efektif. Data untuk visualisasi ini dihasilkan dari perhitungan jumlah transaksi yang mana datanya telah diperoleh sebelumnya. Visualisasi tersebut disajikan dalam bentuk *linechart*, yang menampilkan jumlah tepat indikasi *alert* pada setiap jam. *Trendline* juga ditambahkan untuk memudahkan identifikasi jam-jam yang paling rentan terjadinya *fraud*.



Gambar 3. 44 Visualisasi Data Jumlah *Alert* Berdasarkan Jam

Berdasarkan data visualisasi jumlah *alert* berdasarkan jam dan data transaksi yang telah ditarik, dibuat visualisasi lain mengenai persentase indikasi *fraud* (*alert*) per transaksi berdasarkan jam. Visualisasi ini disajikan dalam bentuk *linechart*, di mana setiap titik mewakili perhitungan persentase jumlah indikasi transaksi *fraud* dibandingkan dengan jumlah total transaksi yang terjadi pada setiap jam. Selain itu, *trendline* juga ditambahkan untuk menunjukkan pada jam berapa sebagian terbesar dari total transaksi memiliki indikasi transaksi *fraud*. Visualisasi yang terbentuk dapat dilihat pada Gambar 3.45 berikut.



Gambar 3. 45 Visualisasi Data Persentase Indikasi *Fraud (Alert)* per Transaksi Berdasarkan Jam

3.3 Kendala yang Ditemukan

Adapun kendala yang ditemukan oleh penulis selama melaksanakan kerja magang pada unit kerja IT Business Enablement di Bank Sahabat Sampoerna adalah sebagai berikut.

1. Kurangnya familiaritas penulis dengan sistem perbankan yang digunakan di perusahaan, seperti T24, Loan Origination System (LOS), Financing Origination System (FOS), dan sebagainya, serta kurangnya pemahaman terhadap berbagai produk atau aplikasi yang ada di Bank Sahabat Sampoerna.
2. Penulis tidak familiar dengan *tool* Google Looker yang digunakan dalam perusahaan untuk pembuatan visualisasi data.
3. Keterbatasan sumber daya yang tersedia untuk menciptakan visualisasi yang lebih menarik, seperti Power BI atau Tableau, yang mungkin dapat meningkatkan kualitas visualisasi yang dihasilkan.

4. Peran yang luas dari posisi IT Business Enablement di Bank Sahabat Sampoerna seperti mencakup tugas yang berkaitan dengan manajemen proyek, perancangan antarmuka sistem, hingga pembuatan visualisasi.

3.4 Solusi atas Kendala yang Ditemukan

Adapun solusi dari kendala yang ditemukan oleh penulis selama melaksanakan kerja magang pada unit kerja IT Business Enablement di Bank Sahabat Sampoerna adalah sebagai berikut.

1. Untuk mengatasi kurangnya familiaritas dengan sistem perbankan yang digunakan dan produk aplikasi Bank Sahabat Sampoerna, penulis meminta penjelasan lebih lanjut dari supervisor serta berusaha mempelajari sistem tersebut melalui tampilan yang tersedia. Selain itu, penulis juga menginstal aplikasi *developer* produk perbankan BSS untuk mencoba-coba dan mempelajari fitur-fitur yang ada.
2. Untuk mengatasi kesulitan dalam menggunakan Google Looker, penulis belajar melalui sumber-sumber dari luar seperti tutorial pada YouTube. Selain itu, penulis juga bertanya kepada rekan yang merupakan anggota dari unit kerja *developer,* yang telah terbiasa menggunakan *tool* tersebut.
3. Untuk mengatasi keterbatasan sumber daya dalam menciptakan visualisasi yang lebih menarik, penulis mencari alternatif solusi dengan mengombinasikan serta memanfaatkan secara kreatif fitur-fitur yang terdapat pada Google Looker.
4. Untuk mengatasi peran yang luas dari posisi IT Business Enablement di Bank Sahabat Sampoerna, penulis belajar melakukan manajemen waktu yang baik. Penulis juga memberikan prioritas pada tugas-tugas utama dan meluangkan waktu untuk menyelesaikan tugas lainnya.