# IDENTIFIKASI TUGAS DAN FUNGSI *DATA STEWARDSHIP* PADA DINAS KOMUNIKASI, INFORMATIKA DAN PERSANDIAN ACEH

**Ima Dwitawati[1)], Putri Nabila [2)], Irfan Mutri Raazi[3)]**
[1)]*Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, ima@ar-raniry.ac.id.*
[2)]*Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, ptriinabilaa01@gmail.com.*
[3)]*Teknologi Informasi, Universitas Islam Negeri Ar-Raniry, Banda Aceh, Irfanmurtiraazi@gamil.com.*
*korespondensi: ima@ar-raniry.ac.id.*

**Abstract**: *In the field of Information Technology, a person who has obligations regarding data security is known as data stewardship (data custodian). Data is the most important part that must be maintained and ensured its security. Therefore, institutions and organizations make various efforts in order to ensure the process of safeguarding and maintaining data, so that the data is safe and can avoid various errors and acts of misuse. This study aims to identify and document the roles, responsibilities and people involved as stewardship data at Diskominfo and Sandi Aceh. Data stewardship is grouped into 4 levels, namely external staff, internal staff, managers of internal institutions, and professionals who support data management. Where each level has specific responsibilities.*
**Keywords:** *Data stewardship, Information Security, Diskominfo dan Sandi Aceh.*

**Abstrak:** Dalam bidang Teknologi Informasi, orang yang memiliki kewajiban tentang pengamanan data dikenal dengan *data stewardship* (penjaga data). Data merupakan bagian terpenting yang harus dijaga dan dipastikan keamanananya. Karenanya, Institusi maupun organisasi melakukan berbagai upaya dalam rangka memastikan proses penjagaan dan pemeliharaan data, sehingga data tersebut aman dan dapat terhindar dari berbagai kesalahan dan tindakan penyalahgunaan. Penelitian ini bertujuan untuk mengidentifikasi dan mendokumentasikan peran, tanggung jawab serta orang yang terlibat sebagai *data stewardship* pada Diskominfo dan Sandi Aceh. *Data stewardship* dikelompokkan kedalam 4 tingkatan yaitu tenaga eksternal, tenaga internal, manajer lembaga internal, dan professional yang mendukung pengelolaan data. Dimana masing-masing tingkatan tersebut memiliki tanggung jawab yang spesifik.
**Kata kunci:** *Data stewardship*, Keamanan Informasi, Diskominfo dan Sandi Aceh.

## 1. Pendahuluan

Keamanan informasi merupakan hal yang sangat penting dalam sebuah instansi terutama pada instansi Dinas Komunikasi, Informatika dan Persandian Aceh. Dinas Komunikasi, Informatika dan Persandian Aceh (Diskominfo dan Sandi Aceh) memiliki sistem informasi yang dapat mengelola keamanan informasi yang bernama sistem informasi laporan keamanan. Sistem informasi ini berguna untuk

melaporkan keamanan dari sebuah sistem dan *email* dari para *user* yang ada terdaftar pada *email* Acehprov.go.id.

Agar sistem informasi ini menjadi lebih efektif, maka dibutuhkan data *email* dari pegawai yang menggunakan *email* Aceh Prov. Data tersebut di simpan pada excel sebelum diinput ke dalam database. Data *email* ini bersifat sensitif karena memuat data pribadi dari pengguna, sehingga harus dijaga kerahasiaannya. Pada saat diberikan data *email* dari sejumlah *user* yang termuat pada *email* Acehprov.go.id, disertai dengan sejumlah instruksi dari pemberi tugas tentang keharusan proses pengamanan data *user*. Instruksi tersebut berupa instruksi lisan.

Dalam bidang Teknologi Informasi, orang yang memiliki kewajiban tentang pengamanan data dikenal dengan *data stewardship* (penjaga data). *Data stewardship* memiliki sejumlah petunjuk atau pedoman dalam rangka kegiatan pengamanan data. Terdapat sejumlah peran dan tanggung jawab dari *data stewardship* yang semestinya dimiliki dan dijabarkan dalam rangka mengamankan data pada suatu organisasi maupun institusi, peran dan tanggung jawab tersebut terdiri dari menentukan sumber data, arbitrase aturan transformasi untuk data, memverifikasi data, berkonstribusi dalam deskripsi bisnis data, mendukung komunitas pengguna data, berkontribusi pada tata kelola program manajemen informasi secara keseluruhan, dan memastikan kualitas data.

Dari ketujuh peran dan tanggung jawab diatas, ditemukan bahwa data yang diinputkan tidak boleh diduplikasi dan disebarluaskan. Namun demikian, *detail* dari teknis pelaksanaan selama melaksanakan Kuliah Kerja Praktek (KKP) belum terdokumentasi secara menyeluruh. Diharapkan identifikasi tugas dan fungsi *data stewardship* ini dapat mendokumentasikan bagaimana peran dan tanggung jawab *data stewardship* dalam menjaga keamanan data *email* pada Diskominfo dan Sandi Aceh.

## 2. Kajian Kepustakaan

### 2.1 Diskominfo dan Sandi Aceh

Dinas Komunikasi, Informatika dan Persandian Aceh (Diskominfo dan Sandi Aceh) adalah perangkat wilayah yang meliputi urusan pemerintahan wilayah pada bidang informasi, komunikasi publik, aplikasi, informatika, persandian serta statistik (Febriani & Juliani, 2022). Berdasarkan Qanun Aceh Nomor 13 Tahun 2016 tentang pembentukan dan penyusunan perangkat Aceh. Dinas Komunikasi, Informatika dan Persandian Aceh merupakan salah satu instansi daerah sebagai unsur pelaksana pemerintah Aceh di bidang komunikasi dan informatika serta mengurus bidang persandian yang bertanggung jawab kepada gubernur Aceh melalui sekretaris daerah.

Dinas Komunikasi, Informatika dan Persandian Aceh mengemban misi utama yaitu menyelenggarakan tugas pemerintahan umum dan pembangunan dibidang komunikasi, informasi, dan persandian. Misi utama Diskominfo dan Sandi Aceh adalah menyelenggarakan tugas pemerintahan umum dan pembangunan dibidang komunikasi, informasi, dan persandian sesuai dengan Pergub Aceh Nomor 55 Tahun 2020 (Dinas Komunikasi Informatika dan Persandian, 2018).

## 2.2 Keamanan Informasi

Keamanan Informasi merupakan penjagaan informasi dari berbagai ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjami n kelangsungan bisnis, meminimalisir resiko bisnis dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis. Keamanan informasi terbagi menjadi lima bagian yaitu:

a) *Physical security* yaitu berupa keamanan yang berfokus pada strategi dalam mengamankan tenaga kerja maupun anggota organisasi, aset fisik, serta lokasi kerja dari sejumlah resiko seperti resiko kebakaran, akses tanpa otorisasi, serta bencana alam.
b) *Personal security* yaitu berupa keamanan yang *overlap* dari *physical security* untuk memberikan perlindungan terhadap individu pada sebuah perusahaan pada sebuah organisasi.

c) *Operational security* yaitu berupa keamanan yang berfokus pada strategi dalam mengamankan kekuatan perusahaan agar tidak ada hambatan saat bekerja.
d) *Communications security* yaitu berupa keamanan dengan tujuan melindungi media komunikasi, teknologi komunikasi dan isinya, serta kecakapan dalam menggunakan alat tersebut agar meraih tujuan suatu perusahaan.
e) *Network security* yaitu berupa keamanan yang berfokus terhadap perlindungan alat jaringan serta organisasi, jaringan serta isinya, dan kecakapan dalam memakai jaringan itu untuk memenuhi fungsi komunikasi data organisasi itu (Nurul et al., 2022).

### 2.3 *Data Stewardship*

*Data stewardship* merupakan serangkaian aktivitas yang bertanggung jawab atas data dan setiap proses yang diperlukan dalam proses pertukaran data (Donge et al., 2022). *Data stewardship* berfokus untuk memastikan bahwa data dapat ditemukan, diakses, diolah, dan digunakan kembali dalam jangka panjang. Termasuk dalam proses pengelolaan data, pengarsipan, dan penggunaan kembali oleh pihak ketiga. Tanggung jawab dari seorang *data stewardship* dimulai dengan memberikan gambaran ilmiah terkait data, kemudian mengumpulkan data, melakukan analisis terhadap data, penyimpanan data, dan pembagian data serta melindungi privasi dari lembaga tersebut. Setiap lembaga memiliki kebijakan, fasilitas, dan keahilan dalam pengelolaan data.

### 2.4 XAMPP (*Cross Platform, Apache, MariaDB, PHP, Perl*)

XAMPP merupakan perangkat lunak bebas, yang mendukung banyak sistem operasi seperti Linux, Windows, MacOs, dan Solaris (Aisy & Iskandar, 2020). XAMPP merupakan kompilasi dari program *Apache*, *MYSQL* (*My Structured Query Language*), *PHP* (*Personal Home Page*), dan *Perl* yang berfungsi sebagai *server* lokal (*localhost*). Dalam XAMPP terdapat komponen utama dengan fungsinya masing-masing, antara lain:

A. XAMPP *Control Panel*, berfungsi untuk mengelola komponen lain pada XAMPP seperti fungsi *Apache, MYSQL, FileZilla, Config, Netstat* serta konfigurasi lainnya.
B. *Htodcs* merupakan komponen XAMPP yang berbentuk *folder*, komponen ini berfungsi sebagai tempat untuk menyimpan *folder* dan *file* yang dapat ditampilkan melalui *browser*. *Htdoc* berada pada *path* C:\xampp\htdocs.
C. *Config*, komponen ini berfungsi sebagai pengaturan dasar seperti mengatur aplikasi *editor text*.
D. *Netstat*, berfungsi untuk melihat *port* yang telah digunakan aplikasi lain.
E. *PhpMyAdmin*, berfungsi untuk mengelola *database* melalui *browser* (Sriwijaya, 2019).

## 3. Metode Penelitian

Metode yang digunakan dalam penelitian ini ialah pendekatan studi kasus serta didukung oleh beberapa referensi pada sumber acuan resmi. Pada penelitian ini dimulai dengan melakukan identifikasi sejumlah *email* yang terdaftar pada acehprov.go.id menggunakan aplikasi berbasis web *server* XAMPP guna memastikan apakah email tersebut masih aktif atau tidak serta menjaga kerahasiaan setiap data *email* yang berisikan tentang sejumlah data pribadi masing-masing pemilik *email* tersebut. Harapannya, junral ini akan memberikan sejumlah saran dan masukan kepada Diskominfo dan Sandi Aceh dalam hal penetapan syarat dan ketentuan dan petunjuk teknis bagi sumber daya yang memiliki tugas dan tanggungjawab dalam hal penjagaan dan pemeliharaan data yang bersifat penting pada suatu instansi maupun institusi. Hal ini diperlukan guna memastikan data perlindungan data atau informasi pemerintah dari kerusakan, kehilangan, penyalahgunaan, dan membuat informasi "layak untuk digunakan".

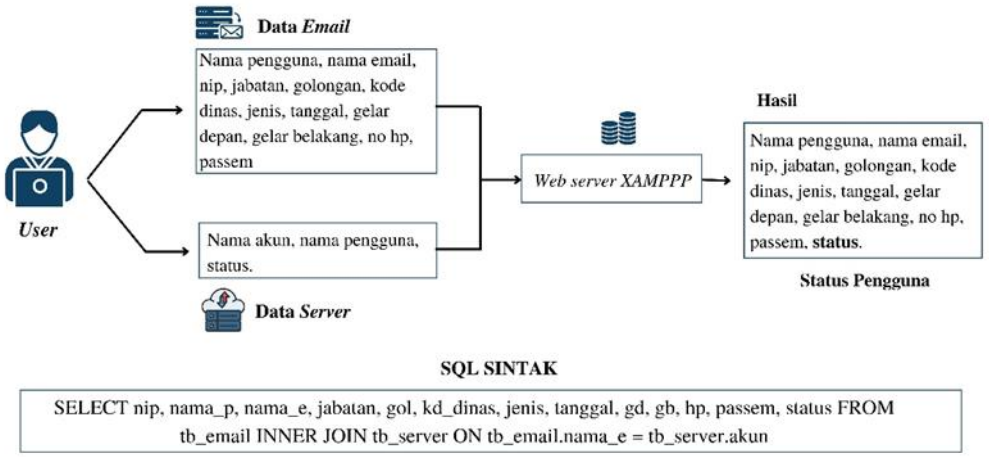
## 4. Hasil dan Pembahasan

### 4.1 Alur Pemrosesan Data

**E-ISSN : 2746-2331**
**P-ISSN : 2746-234X**

Pada tahap ini dilakukan identifikasi data *email* dan data *server* untuk melihat status pengguna aktif atau tidak pada *email* yang terdaftar pada acehprov.go.id. Data yang diberikan sebanyak 5.407 yang tersimpan pada *Microsoft Office Excel.* Pada data *email* tersebut berisikan tentang nama pengguna, nama *email*, Nomor Induk Pegawai (NIP), jabatan, golongan, kode dinas, jenis, tanggal, gelar depan, gelar belakang, no *Handphone* (HP), passem. Sedangkan pada data *server* hanya berisikan akun, nama, dan status. Kedua data tersebut akan dihubungkan untuk melihat status pengguna *email* dengan menggunakan XAMPP.

Gambar 1 memuat sejumlah informasi pribadi dari pemilik akun, maka proses penanganannya memerlukan kehati-hatian, sehingga dapat dipastikan bahwa tidak terjadi penyalahgunaan data maupun tindakan lainnya yang dapat merugikan pemilik data. Instruksi tentang pengamanan ini disampaikan hanya dalam bentuk lisan dari sumber daya yang ada pada instansi tempat melakukan KKP yang ditunjuk sebagai pembina. Dokumentasi instruksi tersebut belum ditemukan secara tertulis, sehingga dalam menjalankannya ada kemungkinan terjadi ketidakkonsistenan ataupun misinterpretasi dari *internship* maupun pegawai yang bertugas melakukan tugas yang sama. Dengan kata lain adalah, belum ditemukannya instruksi tertulis *do* (apa yang boleh) dan *don't* (apa yang tidak boleh) untuk tindakan penanganan setiap data yang diberikan. Selain itu, juga belum ditemukan deskripsi yang lengkap tentang kriteria-kriteria yang harus dipenuhi oleh seorang yang ditugaskan untuk mengamankan data (*data stewardship*).




**Gambar 1.** Alur Proses Data yang Digabungkan Menggunakan Sintak *SQL*

## 4.2 Tanggung Jawab Orang yang Terlibat *Data Stewardship*

Menurut prinsip akuntabilitas dalam *General Data Protection Regulation* (GDPR), lembaga bertanggung jawab untuk memastikan prinsip-prinsip dasar yang berkaitan dengan pemprosesan data pribadi. Setiap lembaga harus menunjuk petugas perlindungan data untuk menjalankan aturan yang dibuat oleh GDPR. Bagi seorang *data stewardship* yang tidak mematuhi prinsip-prinsip tersebut, maka akan mendapatkan konsekuensi berupa rusaknya reputasi, kehilangan kepercayaan, bahkan harus mengembalikan dana hibah untuk lembaga tersebut. *Data stewardship* dalam sebuah lembaga terbagi menjadi 4 bagian yaitu tenaga eksternal, tenaga internal, manajer lembaga internal, dan profesional yang mendukung pengelolaan data (Jansen et al., 2019.).

Tabel 1. Tanggung Jawab Orang Yang Terlibat *Data Stewardship*

| No | Pihak yang Terkait | Tanggung Jawab |
|---|---|---|
| **1.** | Tenaga eksternal | a) Bertanggung jawab atas data penelitian.<br>b) Menggunakan kembali data yang ada.<br>c) Berkolaborasi dengan instansi lain selama penelitian. |

| | | |
|---|---|---|
| | | d) Melindungi privasi dan keamanan subjek data yang dianalisis.<br>e) Menerapkan prinsip data dapat ditemukan, diakses dan dapat digunakan kembali.<br>f) Melindungi kualitas dan reproduktifitas analisis data.<br>g) Menggunakan keahlian yang tersedia dan infrastruktur yang direkomendasikan.<br>h) Berpikir ke depan tentang hak kekayaan intelektual.<br>i) Membagikan data sesuai dengan aturan yang ditetapkan. |
| **2.** | Tenaga internal | a) Mempekerjakan profesional yang menyediakan prosedur dan sistem teknisi pengelolaan data (misalnya manajer data, spesialis Teknologi Informasi (TI), ahli statistik).<br>b) Memiliki manajer lembaga, yang mengatur dan memfasilitasi para professional.<br>c) Memiliki badan pengawas seperti komite peninjau etik data dan petugas privasi.<br>d) Terlibat dengan pihak yang mengumpulkan data.<br>Menawarkan fasilitas untuk melindungi data sesuai dengan oleh GDPR. |
| **3.** | Manajer lembaga internal | a) Menetapkan fasilitas untuk pengelolaan data (misalnya, perlindungan data, penyimpanan, interoperabilitas.<br>b) Menyediakan sarana keuangan untuk pengelolaan data dan tenaga ahli. |

| | | |
|---|---|---|
| | | c) Bertanggung jawab atas organisasi, kebijakan, prosedur standar, dan mengukur kegiatan yang dilakukan.<br>d) Memberikan pembekalan berupa pelatihan bagi pegawai yang bekerja dengan data. |
| **4.** | Profesional yang mendukung pengelolaan data | a) Menyediakan, memberikan saran, dan mendukung penggunaan terminologi, standar TI, dan infrastruktur elektronik yang mempromosikan berbagi dan integrasi data.<br>b) Memberikan saran tentang penulisan bagian dan rencana manajemen data, standar metadata, repositori, dan penanganan data.<br>c) Mendukung kurasi dan pengarsipan data (Jansen et al., 2018). |

Sumber: Jurnal *Research Data Stewardship for Healthcare Professionals*.

### 4.3 Wewenang *Data Stewardship*

Seorang *data stewardship* memiliki beberapa wewenang dalam pengelolaan data. Berikut ini rincian wewenang yang dapat dilakukan oleh seorang *data stewardship*:

**A. Privasi dan Otonomi**

Setiap instansi memiliki suatu privasi dan otonomi orang-orang yang terlibat dalam mengelola data yang mereka punya, berikut ini privasi dan otonomi orang-orang yang terlibat.

**1. Perstujuan yang diinformasikan**

Perstujuan yang diinformasikan berfungsi untuk memberikan informasi subjek studi potensial dari semua aspek partisipasi, termasuk prosedur penanganan data, akses data, dan anonimitas. Wewenang dari seseorang yang diutus instansi dalam menyampaikan informasi ini dapat dengan bebas memutuskan untuk

berpartisipasi atau tidak. Jika mereka ikut berpartisipasi, maka dia akan memahami, menerima resiko dan beban yang terlibat dalam partisipasi itu. Persetujuan yang diiformasikan juga merupakan aspek penting dari GDPR. Terkait dalam pengelolaan data, Persetujuan yang diiformasikan juga harus memenuhi keinginan dari tenaga eksternal yaitu:

a) Penggunaan dan penggunaan kembali data untuk keperluan data saat ini serta yang akan mendatang (termasuk pilihan untuk penyaringan data: data mana yang dapat digunakan untuk penelitian).
b) Pemberitahuan tentang temuan penelitian insidental (perhatian khusus diperlukan untuk hasil yang tidak dapat ditafsirkan sekarang, namun dapat ditafsirkan dalam waktu dekat).
c) Data mana yang berlaku dan dapat diakses.
d) Kemungkinan untuk menarik kembali aspek-aspek tertentu dari persetujuan yang diinformasikan dan konsekuensinya.
e) Data yang digunakan oleh pihak komersial.

**2. Lingkungan perawatan dan penilitian**

Pembeda antara lingkungan perawatan dan lingkungan penelitian ialah pada lingkungan perawatan data yang digunakan untuk diagnosis dan evaluasi dari layananan sebuah instansi. Sedangkan lingkungan penelitian, data yang digunakan nantinya dapat menjawab pertanyaan ilmiah terkait sebuah penelitian. Saat ini, kedua lingkungan data ini semakin terintegrasi. Namun setiap lingkungan data memiliki undang-undang dan pedoman yang berbeda dan dapat saling memperkuat.

**3. Menyiapkan data sensitif untuk digunakan**

Sesuai dengan GDPR, pengelolaan data untuk melakukan penelitian ilmiah atau analisis statistik harus dilindungi sesuai dengan hak dan kebebasan subjek data. pengamanan tersebut harus memastikan setiap instansi memiliki langkah-langkah teknis, terutama untuk memastikan kehormatan terhadapt prinsip minimalisasi data. Setiap data penelitian harus dianonimkan atau disamarkan.

Anonimisasi berarti memproses data dengan tujuan mencegah identifikasi orang yang terkait dengannya secara permanen. Pseudonimisasi berarti mengganti setiap karakteristik pengidentifikasian data dengan nama samaran, yaitu nilai yang tidak memungkinkan orang tersebut untuk diidentifikasi secara langsung. Pseudonimisasi hanya memberikan perlindungan terbatas untuk identitas subjek data karena masih memungkinkan identifikasi menggunakan cara tidak langsung.

**B. Pengumpulan Data**

Pada proses pengumpulan data memiliki dua prinsip utama yaitu memastikan integritas ilmiah data yang dianalisis dan melindungi privasi subjek penelitian dan peneliti untuk memastikan kualitas data, melindungi data dari akses berbahaya, dan menjaga kemampuan untuk menafsirkan data dengan benar. Hal yang dilakukan dalam proses mengumpulkan data sebagai berikut:

**1. Menerapkan infrastruktur manajemen data yang sesuai**

Dengan menerapkan manajemen data, dapat memudahkan dalam bekerja agar lebih fleksibel, mudah, dan cepat. Sistem manajemen data yang digunakan haruslah bersifat professional yang bersertifikat ISO27001, atau setidaknya memenuhi tujuan yang mendasarinya (yaitu, perlindungan, kemampuan akun, privasi, dokumentasi, penilaian risiko, manajemen mutu).

**2. Pemantauan dan validasi**

Untuk melindungi integritas data maka perlunya dilakukan dokumentasi proses entri data secara konsisten seperti siapa dan waktu dalam menginput dan memodifikasi elemen data. Sebelum memutuskan untuk menganalisis data, maka dilakukan validasi dan pembersihan entri data awal untuk mengunci kumpulan data dengan cara meminta pihak instansi untuk data yang dimasukkan, menghasilkan laporan kualitas data, logika konsistensi internal yang luas, entri data ganda, atau dengan membandingkan data dengan sumber utama.

### 3. Metadata

Metadata diartikan sebagai "data tentang data" yang merupakan semua informasi yang diperlukan untuk menafsirkan, memahami, dan menggunakan kembali kumpulan data (Andrian et al., 2021). Metadata dapat disimpan sebagai dokumentasi tertanam, dokumentasi pendukung atau sebagai metadata katalog. Metadata meliputi:

a) Nama kumpulan data atau nama dari proyek data tersebut.
b) Nama dan alamat organisasi atau orang yang membuat data.
c) Nomor identifikasi kumpulan data.
d) Tanggal-tanggal penting yang terkait dengan data, termasuk tanggal mulai dan berakhirnya proyek, tanggal modifikasi data, tanggal rilis, dan periode waktu yang dicakup oleh data.
e) Deskripsi asal data yang telah diverifikasi.
f) Protokol yang digunakan termasuk aspek eksperimental dan pengaturan studi (misalnya, orang, prosedur operasi standar, kondisi, pengaturan instrumen, data kalibrasi, filter data, dan pemilihan subset data), hal ini penting untuk penggunaan kembali data dan verifikasi kualitas data.

## C. Keamanan

Langkah-langkah dalam pengamanan data sebagai berikut:

### 1. Kebijakan akses

Sebelum proses pengumpulan data, pentingnya memiliki kebijakan akses yaitu tidak mengizinkan akses ke data pribadi atau klinis kepada orang yang tidak berwenang, dalam keadaan apa pun memberikan akses ke dalam data yang dapat diidentifikasi secara langsung, menggunakan metode selain kemanan kata sandi ('otentikasi 2-faktor'), dan memastikan bahwa akses ke *database* dicatat dengan benar.

### 2. Melindungi data penelitian

Langkah-langkah yang dibutuhkan untuk melindungi data yaitu, penyimpanan data penelitian harus dijaga terutama berdasarkan peraturan yang berlaku di Indoneisa. Sistem dan lingkungannya sebaiknya bersertifikat ISO27001 atau setidaknya memenuhi tujuan yang mendasari undang-undang. Seorang manajer *database* harus dapat membedakan akses data pada bagian-bagian tertentu. Basis data yang terhubung ke internet tidak boleh berisi data yang dapat diidentifikasi kecuali infrastruktur telah mengambil langkah-langkah yang memadai untuk mengurangi risiko akses ke identitas subjek ke tingkat yang sangat rendah. Dan penyimpanan yang secara legal dapat dilacak kembali.

## D. Menganalisis Data

Sebelum melakukan analisis data, hal yang harus dipersiapkan sebagai berikut:

### 1. Persiapan data mentah

Persiapan data dimulai dengan membuat kamus data (metadata), membuat file analisis dan salinan dataset agar arsipkan data mentah terjaga dengan aman, dokumentasikan semua langkah pembersihan secara terpisah file yang diarsipkan.

### 2. Rencana Analisis

Sebelum analisis data dimulai, maka dibutuhkan pembahasan mengenai pertanyaan penelitian dalam hal populasi, intervensi, perbandingan, dan hasil. Deskripsi sub kelompok dari populasi yang akan dimasukkan dalam analisis. Kumpulan data yang digunakan kemudian bagaimana kumpulan data digabungkan. Kategori variable yang digunakan. Perlakuan terhadap nilai yang hilang kemudian urutan dalam melakukan analisis dan penataan folder dan file serta mengelola control versi file.

## E. Pengarsipan Data

E-ISSN : 2746-2331
P-ISSN : 2746-234X

Terdapat banyak metode yang dapat dilakukan dalam melakukan pengarsipan data salah satunya dengan melakukan pengarsipan secara publik yaitu dengan disiplin ilmu, jurnal ilmiah, dan penyandang data penelitian. Setiap instansi harus mengarsipkan data pada instansi masing-masing pada repositori yang mereka miliki. Apabila data yang diarsipkan di luar institusi seperti layanan data internasional atau repositori domain harus didaftarkan terlebih dahulu pada institusi pemilik data dan data tersebut harus terdaftar dalam katalog data terbuka.

## F. Berbagi Data

Prinsip dalam berbagi data harus dilakukan secara bertanggung jawab dan melindungi privasi subjek data yang akan dilakukan analisis. Berikut ini prinsip-prinsip yang harus dimiliki dalam melakukan berbagi data:

### 1. Pertimbangan Umum

Kebijakan berbagi data dipengaruhi oleh pertanyaan-pertanyaan berikut:

a) Apakah subjek penelitian memberikan izin untuk berbagi atau menggabungkan data mereka? Apakah persetujuan menyebutkan ketentuan khusus untuk berbagi data?
b) Bagaimana data dibuat dan bagaimana hal ini memengaruhi pembagian data (misalnya, metodologi, protokol, dan publikasi)?
c) Jenis data apa yang akan dirilis? Apakah ada prosedur untuk rilis data dengan, misalnya, sebuah komite?
d) Siapa yang akan menjadi penerima data?
e) Jaminan apa yang akan diberikan penerima tentang penggunaan data yang bertanggung jawab?

Akses eksternal biasanya bersifat terbatas (akses terbartas). Jika data yang diperoleh merupakan data kolaborasi, hak kekayaan intelektual dan keterbukaan data yang dihasilkan harus didiskusikan di antara para mitra sebelum Anda mulai mengumpulkan data. Berikut ini faktor yang harus dipenuhi:

a) Modalitas persetujuan (yaitu, apakah ada persetujuan yang diinformasikan dan apa yang dinyatakannya?).
b) Persetujuan penelitian oleh badan kompeten yang ditunjuk.
c) Kondisi penyandang dana data penelitian.
d) Kondisi di mana data dirilis oleh pembuat asli data.
e) Kondisi jurnal tempat data dikirimkan (semakin banyak jurnal yang menuntut akses terbuka ke data yang mendasarinya).

**2. Berbagi dengan pihak komersial**

Data hanya dapat dibagikan dengan pihak komersial eksternal jika pemilik data telah memberikan persetujuan untuk memberikan akses. Tenaga eksternal tidak boleh menyerahkan hak eksklusif untuk menggunakan kembali atau mempublikasikan data kepada penerbit atau agen komersial tanpa mempertahankan hak untuk membuat data tersebut tersedia secara terbuka untuk digunakan kembali.

Dengan adanya *data stewardship* dapat membantu Diskominfo dan sandi Aceh dalam membuat kebijakan untuk pengamanan data serta dapat memberikan akses yang sesuai, khususnya bagi tenaga eksternal seperti para peserta magang agar tidak terjadi penyalahgunaan data tersebut.

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

Berdasarkan uraian pada bagian sebelumnya, maka dapat disimpulkan hal-hal sebagai berikut:

1. Data merupakan bagian terpenting yang harus dijaga dan dipastikan keamanananya. Karenanya, Institusi maupun organisasi melakukan berbagai upaya dalam rangka memastikan proses penjagaan dan pemeliharaan data, sehingga data tersebut aman dan dapat terhindar dari berbagai kesalahan dan tindakan penyalahgunaan.

2. Salah satu tindakan yang dapat dilakukan oleh institusi maupun organisasi dalam rangka pengamanan data adalah dengan menetapkan peran dan tanggung jawab secara tertulis yang dilengkapi dengan petunjuk tentang apa yang boleh (*do*) dan apa yang tidak boleh (*don't*) dilakukan oleh seorang penjaga data (*data stewardship*).
3. *Data stewardship* memiliki tanggung jawab yang dikelompokkan kedalam 4 tingkatan, tenaga eksternal, tenaga internal, manajer lembaga internal, dan professional yang mendukung pengelolaan data. Dimana masing-masing tingkatan tersebut memiliki tanggung jawab yang spesifik.

## 5.2 Saran

Berdasarkan kesimpulan dan hasil pembahasan yang telah diuraikan diatas, maka dalam penelitian ini disarankan:

1. Institusi maupun organisasi sebaiknya menunjuk seorang penjaga data (*data stewardship*) yang bertanggung jawab untuk menjaga keamanan data yang ada pada institusi tersebut.
2. Seorang *data stewardship* sebaiknya dilengkapi dengan pedoman tentang bagaimana ia melakukan proses penanganan dan pengamanan data yang ada dalam wilayah kerjanya.

## Daftar Kepustakaan

Aisy, B. I., & Iskandar, A. (2020). Perancangan Sistem Monitoring Pekerjaan Survey Digitalisasi SPBU Pertamina Berbasis Web. *EJournal Mahasiswa Akademi Telkom Jakarta (EMIT)*, *2*(1), 19–26.

Andrian, D. P. E., Fudholi, D. H., & Prayudi, Y. (2021). Karakteristik Metadata Pada Sharing File Di Media Sosial Untuk Mendukung Analisis Bukti Digital. *Jurnal Ilmiah SINUS*, *19*(1), 13. https://doi.org/10.30646/sinus.v19i1.494

Dinas Komunikasi Informatika dan Persandian. (2018). Dinas komunikasi informatika dan persandian. *Dinas Komunikasi Informatika Dan Persandian*,

*14*.

Donge, W. Van, Bharosa, N., & Janssen, M. (2022). *Informasi Pemerintah Triwulanan Pemerintah berbasis data : Perbandingan lintas kasus pengelolaan data dalam ekosistem data*. *39*(September 2021).

Febriani, D. L., & Juliani, R. (2022). Strategi Komunikasi Pemerintah Daerah Dalam Mensosialisasikan Informasi Publik Di Kabupaten Aceh Barat. *At-Tanzir: Jurnal Ilmiah Prodi Komunikasi Penyiaran Islam*, 19–38. https://doi.org/10.47498/tanzir.v13i1.970

Jansen, P., van den Berg, L., van Overveld, P., & Boiten, J. W. (2018). Research data stewardship for healthcare professionals. *Fundamentals of Clinical Data Science*, 37–53. https://doi.org/10.1007/978-3-319-99713-1_4

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi : Keamanan Informasi , Teknologi Informasi Dan Network ( Literature Review Sim ). *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, *3*(5), 564–573.

Sriwijaya, P. N. (2019). BAB II Tinjauan Pustaka BAB II TINJAUAN PUSTAKA 2.1. 1–64. *Gastronomía Ecuatoriana y Turismo Local.*, *1*(69), 5–24.