

REGULASI PERDAGANGAN TERKAIT PERLINDUNGAN PRIVASI KONSUMEN DALAM EKSPANSI BISNIS DI UNI EROPA: STUDI KASUS ALIBABA

Gracella Leonora¹⁾, Roy Vincentius Pratikno²⁾

*Alumni, Fakultas Ilmu Sosial dan Ilmu Politik, Program Studi Hubungan Internasional, Universitas Pelita Harapan
Fakultas Ilmu Sosial dan Ilmu Politik, Program Studi Hubungan Internasional, Universitas Pelita Harapan*

e-mail: 01043200007@student.uph.edu¹⁾, roy.pratkno@lecturer.uph.edu²⁾

ABSTRAK

Uni Eropa menetapkan regulasi perdagangan yang ketat, khususnya terkait perlindungan privasi konsumen yang diatur oleh *General Data Protection Regulation* (GDPR). Negara/organisasi yang menghadapi masalah privasi atau tidak memiliki standar perlindungan data yang memadai, harus menghadapi hambatan dalam ekspansi bisnis di Uni Eropa. Melalui studi kasus Alibaba, penelitian ini secara khusus menganalisis tantangan dan strategi kepatuhan GDPR pada ekspansi bisnis di Uni Eropa. Penelitian ini dilakukan untuk menyelidiki penerapan GDPR di Uni Eropa dan menganalisis seluruh strategi dan tindakan yang ditempuh Alibaba untuk mematuhi GDPR. Kerangka dari penelitian ini adalah teori Neoliberalisme, juga berlandaskan konsep perdagangan internasional, konsep privasi dan data pribadi, konsep otoritas publik, dan konsep perusahaan multinasional. Penelitian ini menggunakan pendekatan kualitatif dengan metode penelitian deskriptif dan studi kasus. Data diperoleh dari data sekunder. Kemudian, dianalisis menggunakan teknik analisis naratif. Penelitian ini menganalisis hubungan ekonomi antara Uni Eropa dan Tiongkok sebagai latar belakang, kemudian mengulas perkembangan regulasi perlindungan privasi konsumen di Uni Eropa, dan menganalisis strategi Alibaba ekspansi di Uni Eropa. Berdasarkan hasil dari penelitian yang dilakukan, GDPR tidak mengizinkan negara/perusahaan yang memiliki masalah privasi dan tidak memiliki perlindungan data yang memadai untuk beroperasi di Uni Eropa. Sebagai perusahaan yang memenuhi kriteria pelanggaran tersebut, Alibaba berhasil ekspansi di Uni Eropa dengan memperbaiki masalah internal dan membentuk regulasi yang sesuai GDPR di setiap anak perusahaannya.

Kata kunci: Uni Eropa, Alibaba, GDPR, Tiongkok, Privasi

ABSTRACT

The European Union (EU) has implemented stringent trade regulations, particularly regarding consumer privacy protection governed by the General Data Protection Regulation (GDPR). Countries or organizations facing privacy issues or lacking adequate data protection standards must encounter barriers in business expansion in the EU. Through a case study of Alibaba, this research specifically analyzes the challenges and GDPR compliance strategies in business expansion within the European Union. The study investigates the implementation of GDPR in the EU and analyzes all the strategies and actions taken by Alibaba to comply with GDPR. The research framework is based on Neoliberalism theory, as well as international trade concepts, privacy and personal data concepts, public authority concepts, and multinational corporation concepts. The research employs a qualitative approach with descriptive research methods and a case study. Data were obtained from secondary sources and analyzed using narrative analysis techniques. The study analyzes the economic relationship between the EU and China as a background, reviews the development of consumer privacy protection regulations in the EU, and analyzes Alibaba's expansion strategy in the EU. Based on the research findings, GDPR does not allow countries/companies with privacy issues and inadequate data protection to operate in the EU. As a company meeting these violation criteria, Alibaba successfully expanded in the EU by addressing internal issues and establishing regulations compliant with GDPR in each of its subsidiaries.

Keywords: European Union, Alibaba, GDPR, China, Privacy

1. Pendahuluan

Dengan kemajuan teknologi, khususnya melalui internet, perdagangan internasional semakin terintegrasi melalui berbagai platform digital. Salah satu yang paling populer dan berkembang pesat saat ini adalah perdagangan elektronik atau yang umumnya dikenal sebagai *e-commerce* (Terzi, 2011). *E-commerce* melibatkan transfer dana secara daring, pertukaran data elektronik, serta pengelolaan sistem secara otomatis (Simamora, 2017). Selain itu, *e-commerce* juga memfasilitasi transaksi komersial yang melintasi batas negara dengan lebih efisien dan ekonomis daripada sistem perdagangan tradisional tradisional. Namun, sisi negatif dari perkembangan *e-commerce* adalah adanya kekhawatiran terkait pengumpulan dan pengelolaan data pribadi yang dapat mengancam privasi konsumen (Muneer & Farooq, 2018). Sebab, aktivitas dan informasi konsumen sering kali dikumpulkan dan disimpan oleh platform digital, dan apabila platform tersebut tidak memiliki perlindungan yang memadai, data-data konsumen dapat digunakan oleh pihak-pihak yang tidak bertanggung jawab. Dengan kurangnya pertemuan langsung antara penjual dan pembeli, informasi pribadi yang dikumpulkan platform digital menjadi perhatian utama, yang pada gilirannya meningkatkan kesadaran masyarakat terhadap isu privasi (Wiranjaya & Ariana, 2017). Privasi konsumen sangat berpengaruh pada pertumbuhan perdagangan digital suatu negara. Menjaga privasi konsumen adalah elemen penting dalam membangun fondasi kepercayaan yang diperlukan untuk pertumbuhan perdagangan digital antarnegara (Rosadi & Pratama, 2018). Sebagai respons terhadap kebutuhan akan keamanan, diperlukan pembentukan regulasi perdagangan yang fokus pada perlindungan privasi konsumen.

Uni Eropa sebagai salah satu entitas perdagangan terkemuka di dunia, memainkan peran penting dalam membentuk ilustrasi perdagangan

internasional. Sehingga, tidak heran Uni Eropa menjadi sasaran pasar potensial bagi perusahaan asing, khususnya *e-commerce* untuk mengembangkan usaha. Beberapa faktor yang membuat Uni Eropa menjadi pasar yang potensial adalah populasi, dengan jumlah sekitar 446 juta penduduk pada tahun 2022 dengan beragam budaya dan preferensi konsumen, membuat Uni Eropa sebagai pasar yang menarik bagi perusahaan *e-commerce* (O'Neill, 2023). Faktor kedua, tingkat pengeluaran konsumen di Uni Eropa relatif tinggi. Trading Economics menunjukkan peningkatan pengeluaran konsumen dari 1798,74 miliar EUR pada kuartal pertama tahun 2023 menjadi 1799,44 miliar EUR pada kuartal kedua tahun 2023 (EUROSTAT, 2023). Faktor ketiga, ketatnya regulasi perdagangan di Uni Eropa, baik yang berlaku secara nasional maupun internasional dalam hal melindungi privasi konsumen (Schoukens & Bastmeijer, 2014) yang dituangkan dalam *General Data Protection Regulation* (GDPR) sehingga menjamin perusahaan *e-commerce* untuk membangun reputasi yang baik dan memberikan perlindungan privasi yang kuat kepada konsumen.

Namun sebaliknya, regulasi ini membuat Perusahaan asing dihadapkan pada prosedur yang tidak mudah mencakup tinjauan latar belakang dan penilaian yang dilakukan oleh beberapa negara anggota Uni Eropa (Hess & Mariottini, 2015). Selain itu, GDPR sendiri menerapkan prosedur ketat bagi perusahaan asing yang mengumpulkan data pribadi dari penduduk Uni Eropa. Negara atau perusahaan yang memiliki masalah privasi atau tidak memiliki perlindungan data yang memadai, dilarang untuk mengakses data pribadi penduduk setempat (GDPR, 2018).

Pemilihan Alibaba sebagai studi kasus karena Alibaba memenuhi kriteria pelanggaran yang ditegakkan oleh GDPR. Kriteria pertama, Alibaba berasal dari Tiongkok, yang memiliki regulasi perlindungan data yang relatif lebih longgar

dibandingkan dengan Uni Eropa. Kedua, Alibaba menghadapi tantangan terkait keamanan data konsumen yang bocor dalam anak perusahaannya. Diantaranya, Alibaba Cloud terlibat dalam kasus pencurian basis data polisi Shanghai dan pencurian data satu miliar warga Tiongkok. Para ahli data di dunia maya mengonfirmasi bahwa data-data tersebut disimpan di server Alibaba Cloud tanpa perlindungan kata sandi selama 14 bulan. (Partridge, 2022). Dan beberapa beberapa kasus, server di Tiongkok diretas dan data masyarakat diperjualbelikan secara ilegal (Goh, 2022). Selain itu ElasticSearch, tempat penyimpanan data milik Departemen Keamanan Publik Provinsi Jiangsu, menyimpan 90 juta informasi pribadi tanpa perlindungan dan membocorkan 13,7 juta data pengguna. Tidak hanya itu, pada akhir tahun 2020 data pribadi dari 1,95 juta anggota Partai Komunis Tiongkok juga mengalami kebocoran di platform digital (Bisson, 2023). Dengan kasus-kasus tersebut, menjadi alasan Alibaba memenuhi dua kriteria pelanggaran GDPR untuk beroperasi di Uni Eropa. Dua kriteria tersebut menjadi penghalang bagi Alibaba untuk mendapatkan izin masuk dan mengakses data konsumen di Uni Eropa.

Keberhasilan Alibaba memasuki pasar dan bahkan mengalami pertumbuhan yang pesat di Uni Eropa (Kharpal, 2023) dan membangun Electronic World Trade Platform (eWTP) di Belgia dan mendirikan kantor Alibaba di Jerman dan Perancis (Millward, 2015) menarik untuk dikaji.

2. Tinjauan Pustaka

2.1. Perlindungan Privasi dan Data Konsumen di E-Commerce

Bersamaan dengan pertumbuhan *e-commerce*, terdapat pengelolaan dan penyimpanan jutaan data pribadi konsumen yang dilakukan oleh pedagang *online*. Stephen Fienberg menegaskan bahwa di dalam lingkup *e-commerce*, data *mining* beroperasi dalam kerangka yang tidak mengabaikan privasi individu. (Fienberg,

2006). Namun, ketika data individu yang digunakan oleh para penjual *e-commerce* dikaitkan dengan basis data lain, maka aspek privasi konsumen menjadi hal penting yang perlu diperhatikan. Situasi ini memunculkan pertanyaan tentang privasi data dan kepercayaan, yang pada gilirannya menyebabkan kekhawatiran di kalangan konsumen. Pernyataan tersebut diperkuat oleh temuan Bettina Berendt, Oliver Günther, dan Sarah Spiekermann, di mana saat menjelajahi situs *e-commerce* sebanyak 75% pengguna internet di Jerman merasa khawatir terhadap data privasi, dan sekitar 30-40% diantaranya memberikan informasi palsu dan tidak jujur ketika dimintai data mengenai kebiasaan serta preferensi pribadi secara daring (Gunther, Spiekermann, & Berendt, 2005) Seiring dengan pendapat tersebut, Ackerman, Lorrie Faith Cranor, dan Joseph Reagle menguraikan dalam penelitiannya responden menunjukkan tingkat kekhawatiran yang tinggi mengenai privasi di internet yang disebabkan oleh kurangnya pengetahuan dan kepercayaan terhadap praktik pengelolaan informasi yang dilakukan oleh perusahaan *e-commerce* (Ackerman, Cranor, & Reagle, 1999).

Salah satu hasil utama yang dapat disimpulkan dari kedua penelitian tersebut adalah konsumen yang berpartisipasi dalam interaksi daring seringkali tidak memiliki kendali penuh atas tindakannya, sehingga konsumen cenderung mengandalkan perlindungan hukum. Mark Budnitz menjelaskan bahwa konsumen yang terlibat dalam perdagangan elektronik dengan sektor swasta memerlukan perlindungan hukum (Budnitz, 1998). Tanpa regulasi yang memberikan perlindungan privasi, konsumen menghadapi risiko besar terhadap pelanggaran data dan privasinya. Selain itu, perusahaan juga sangat memerlukan regulasi tersebut karena banyak konsumen mungkin akan menolak terlibat dalam *e-commerce*, sehingga dapat mengurangi volume bisnis yang diperlukan industri untuk mencapai profitabilitas.

Dengan kata lain, seperti yang diungkapkan oleh Mark Budnitz, keberhasilan *e-commerce* sangat bergantung pada kemampuannya untuk memperoleh kepercayaan konsumen, yang seringkali hanya dapat dicapai melalui keberadaan perlindungan hukum yang berkaitan dengan privasi konsumen.

2.2. Perbandingan Regulasi Perlindungan Privasi Konsumen di Tiongkok dan Uni Eropa

Terdapat perbedaan regulasi perdagangan yang cukup signifikan antara Tiongkok dengan Uni Eropa. Uni Eropa disatu sisi memiliki regulasi yang kuat dalam perlindungan privasi konsumen, termasuk perlindungan terhadap praktik perdagangan yang tidak adil, keselamatan produk, informasi konsumen, dan hak konsumen sedangkan Tiongkok, dalam praktik penerapan undang-undang perlindungan privasi konsumen masih lemah dan perlu peningkatan lebih lanjut. Seperti yang ditunjukkan dalam tulisan perbandingan tersebut, sistem Tiongkok dan Uni Eropa tampak berbeda secara substansial, namun tinjauan yang lebih mendalam mengungkapkan adanya kecenderungan konvergensi antara kedua sistem tersebut. (Binding & Purnhagen, 2011; Lin, 2021). Konvergensi tersebut mencakup penyalarsan regulasi, penanganan praktik perdagangan yang tidak adil, dan peningkatan hak konsumen. Meskipun saat ini terdapat perbedaan dalam tingkat kekuatan regulasi, adanya konvergensi mencerminkan upaya kedua wilayah tersebut untuk menyesuaikan diri dengan standar internasional dan memperkuat perlindungan privasi konsumen dalam era digital. Di Uni Eropa, masalah penegakan hukum dan perlindungan privasi konsumen diakui dalam praktiknya, sehingga mengarah pada pendekatan gabungan antara penegakan swasta dan pengawasan berbasis negara terhadap pasar, dengan memanfaatkan kekuatan persaingan pasar. Di sisi lain,

Tiongkok telah mengkualifikasi perlindungan privasi konsumen sebagai kebijakan negara yang tidak dapat ditinggalkan kepada penegakan individu, karena ketidaksempurnaan pasar dapat menyebabkan ketidakpercayaan yang tidak diinginkan oleh konsumen dan pengembangan pasar dan produksi. Namun, penegakan individu dan pengawasan oleh negara telah ditingkatkan dalam beberapa tahun terakhir sehingga dapat dikatakan bahwa beberapa elemen penegakan swasta Uni Eropa juga dapat diidentifikasi dalam sistem Tiongkok. Dari kedua perbandingan tersebut, dapat disimpulkan bahwa beberapa keputusan pemerintah Tiongkok untuk mengenalkan langkah-langkah regulasi dan pembatasan yang mempengaruhi bidang *e-commerce* didasarkan pada pertimbangan keamanan nasional. Berbeda dengan peraturan hukum Uni Eropa, dalam bidang *e-commerce* di Tiongkok, terdapat pembatasan tertentu yang terkait dengan isu-isu menjaga keamanan nasional (Lin, 2021).

Uni Eropa memiliki kerangka hukum yang mengatur hak-hak konsumen di seluruh wilayahnya. Tujuan kebijakan konsumen Uni Eropa adalah menjadi kenyataan yang nyata bagi 500 juta warga negaranya dengan menjamin hak-hak mereka sebagai konsumen. Hal tersebut berarti melindungi konsumen dari risiko serius dan ancaman yang tidak dapat mereka hadapi secara individu, memberdayakan mereka untuk membuat pilihan berdasarkan informasi yang akurat, jelas, dan konsisten, meningkatkan kesejahteraan mereka dan melindungi keamanan serta kepentingan ekonomi mereka dengan efektif. Undang-undang yang diadopsi di tingkat Uni Eropa bertujuan terutama untuk melindungi kepentingan keselamatan, kesehatan, ekonomi, dan hukum konsumen, serta menawarkan jaminan dan sistem keselamatan produk secara umum. Instrumen hukum khusus yang banyak digunakan oleh Uni Eropa dalam bidang

perlindungan privasi konsumen adalah direktif. Mengingat tingkat perlindungan data pribadi yang berbeda di negara-negara anggota, Uni Eropa menetapkan Direktif ini untuk menyatukan tingkat perlindungan tersebut. Salah satu fitur utama dari Direktif ini adalah bahwa cakupan perlindungan diperluas ke data manual. Ada dua tujuan dasar dari Direktif ini, pertama, melindungi hak dan kebebasan dasar individu, terutama hak privasi mereka; kedua, memastikan bahwa informasi mengalir secara bebas di negara-negara anggota sesuai dengan prinsip-prinsip umum aliran bebas barang dan jasa. Saat ini, dasar hukum untuk perlindungan privasi di industri *e-commerce* Tiongkok dan lingkungan sosial yang lemah, sehingga perlindungan privasi konsumen dengan baik tanpa merugikan perkembangan normal industri *e-commerce* telah menjadi masalah hukum yang mendesak untuk diatasi (Guo, 2021) konstitusi, hukum sipil, hukum administrasi, hukum pidana, dan hukum acara serta undang-undang di Tiongkok lainnya tidak memiliki ketentuan hukum yang secara langsung mengatur privasi dan mengatur tanggung jawab operator jaringan serta hukuman bagi pelaku yang melanggar, sehingga bidang pengawasan sulit melaksanakan tugas pengawasannya (Yang, 2011).

2.3. Ekspansi Perusahaan Tiongkok di Uni Eropa

Ekspansi perusahaan Tiongkok di Uni Eropa menunjukkan komitmennya untuk beroperasi di pasar global dan menghadapi persaingan secara internasional. Dengan memahami tantangan dan peluang yang ada, perusahaan Tiongkok dapat berhasil memperluas jangkauan bisnisnya dan mengambil bagian dalam pertumbuhan ekonomi di Uni Eropa. Perusahaan milik negara Tiongkok dan instrumen keuangan memfasilitasi pelaksanaan *soft power* Tiongkok dan eksekusi strategi besar-besaran negara tersebut. Investasi Tiongkok

memberikan jaringan hubungan komersial yang semakin padat, melalui mana Tiongkok memperluas cakupan dan jangkauan pengaruhnya serta proyeksi kekuasaannya dengan implikasi bagi sistem internasional (Ishmael, 2020).

Benua Eropa menduduki peringkat pertama sebagai tujuan investasi Tiongkok. Investasi Tiongkok di benua ini mencakup berbagai sektor, mulai dari infrastruktur skala besar di sebagian Eropa Selatan dan Tenggara hingga perusahaan teknologi tinggi di bagian barat benua (Vecchi & Brennan, 2022). Kasus Alibaba menunjukkan bahwa model ekosistem bisnis, teknologi komputasi data, merek yang kuat, visi pendiri, hubungan dengan pemimpin politik di berbagai negara, dan kualitas produk dan layanan adalah keunggulan kompetitifnya. Model ekosistem bisnis Alibaba memungkinkan perusahaan memperoleh titik pertumbuhan pendapatan baru di pasar Tiongkok dan internasional. Teknologi Ali Cloud merupakan dasar dari model bisnis Alibaba. Itulah mengapa keunggulan kompetitif muncul. Teknologi unik ini memungkinkan Alibaba masuk ke pasar lain tanpa kehilangan keunggulan teknologinya. Keunggulan kepemilikan tak berwujud lainnya dari Alibaba adalah efek mereknya yang semakin kuat secara global dan membantu bisnis-bisnis baru masuk ke wilayah baru dengan mudah (Wang, 2018).

3. Metode Penelitian

Penelitian ini dikaji dengan pendekatan kualitatif, pendekatan ini sesuai dengan kebutuhan terhadap kajian kebijakan perdagangan terkait perlindungan privasi konsumen dalam ekspansi bisnis di Uni Eropa, dan memanfaatkan data literatur, berupa buku, jurnal, dan laporan tertulis lainnya. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian deskriptif dan studi kasus. Kedua metode ini digunakan untuk mengidentifikasi alur perkembangan perlindungan data di Uni Eropa hingga

menjadi regulasi global yang wajib ditaati oleh perusahaan asing yang beroperasi di wilayah tersebut. Penelitian ini memanfaatkan sumber data sekunder yang dikumpulkan melalui studi kepustakaan dan penelusuran daring. Pada proses analisis data menggunakan teknik analisis naratif sebagai gaya penulisannya. Oleh karena itu, dengan teknik ini peneliti akan menggali tantangan regulasi perdagangan terkait perlindungan privasi konsumen dalam ekspansi bisnis di Uni Eropa, dengan studi kasus pada perusahaan Alibaba.

4. Hasil dan Pembahasan

4.1. GDPR

Uni Eropa meningkatkan dan memperluas kerangka hukum perlindungan data dengan mengadopsi General Data Protection Regulation (GDPR). GDPR hadir sebagai kerangka kerja yang lebih seragam dan konsisten di seluruh Uni Eropa. Dengan demikian, GDPR mencerminkan upaya pemerintah untuk memperkuat kerangka hukum dalam menghadapi tantangan baru yang muncul dalam pengelolaan data pribadi secara global. GDPR secara resmi diadopsi sebagai undang-undang pada bulan Mei 2016. Namun, aturan ini mulai berlaku dan efektif pada tanggal 25 Mei 2018 (Hoofnagle, Van Der Sloot, & Borgesius, 2023). GDPR adalah undang-undang perlindungan data yang menetapkan aturan untuk memproses, menyimpan, dan mengelola data penduduk Uni Eropa yang tinggal di dalam maupun luar Uni Eropa. Meskipun demikian, dampak GDPR bersifat global sehingga dapat memengaruhi setiap organisasi/perusahaan yang menargetkan pasar Uni Eropa sebagai tempat beroperasi dan menyediakan barang/layanan kepada penduduk setempat. GDPR juga mengikat semua negara anggota Uni Eropa tanpa memerlukan implementasi undang-undang di tingkat nasional. Perubahan-perubahan tersebut kemudian disusun menjadi 99 pasal. GDPR memberikan definisi yang lebih spesifik

dengan cakupan luas sesuai perkembangan teknologi saat ini. Selain identifikasi langsung, GDPR juga mencakup identifikasi yang dapat dilakukan dengan menggunakan identitas *online*, karakteristik fisik, fisiologis, genetik, mental, ekonomi, budaya, dan sosial individu (GDPR, art. 4 (1)). Data-data tersebut mencakup detail pribadi, seperti nama, alamat email, nomor keamanan sosial, alamat IP, nomor telepon, tanggal lahir, data geolokasi, dan data biometrik seperti *cookies*. Sementara itu, GDPR mendefinisikan “pengolahan data” sebagai rangkaian operasi yang dilakukan pada data pribadi secara manual atau dengan bantuan teknologi (GDPR, art. 4(2) dan 4 (5)). Aktivitas pengolahan data meliputi, pengumpulan, pencatatan, organisasi, struktur, penyimpanan, adaptasi atau perubahan, pengambilan, konsultasi, penggunaan, pengungkapan melalui transmisi, penyebaran dan penghapusan data pribadi. Oleh karena itu, seluruh tindakan yang melibatkan data pribadi akan dianggap sebagai pengolahan dan harus tunduk pada GDPR.

Dalam menerapkan sanksi GDPR, terdapat sebuah otoritas yang disebut *Data Protection Authorities* (DPAs) dari masing-masing negara anggota yang berwenang untuk menegakkan regulasi tersebut. GDPR juga mengharuskan organisasi/perusahaan untuk menunjuk seorang perwakilan sebagai penghubung komunikasi antara pengendali dengan subjek data dan otoritas pengawasan data (GDPR, art. 51). Dalam GDPR, sanksi berlaku untuk setiap organisasi/perusahaan, tanpa memandang ukuran, jenis, atau kewarganegaraan yang mengumpulkan atau memproses data pribadi dari individu yang berada di Uni Eropa dan *European Economic Area*. Sanksi yang diberikan DPAs mencakup aspek finansial yang bersifat administratif dan regulatif (Voss & Dumas, 2021).

4.2. Pengaruh GDPR terhadap Transfer Data Pribadi ke Negara Ketiga dan Perusahaan Asing yang beroperasi di Uni Eropa

Salah satu tantangan utama GDPR dalam konteks global adalah cara data pribadi dengan mudah dipindahkan ke negara ketiga. Terutama, jika tempat tersebut dianggap sebagai *data haven* (Hoofnagle, Van Der Sloot, & Borgesius, 2023). *Data haven* menjadi sumber kekhawatiran dalam keamanan data, sebab pengendali data memindahkan data pribadi ke negara yang lemah akan perlindungan privasi. Hal ini tentunya dapat meningkatkan risiko ancaman bagi privasi individu, khususnya di dalam Uni Eropa. Oleh karena itu, GDPR membentuk kerangka kerja atau struktur yang terorganisir untuk mengatur transfer data internasional (GDPR, art.44). Aturan-aturan tersebut dijelaskan secara ringkas, sebagai berikut:

1. European Commission memiliki wewenang untuk mengevaluasi hukum negara lain dan menentukan negara tersebut memadai atau tidak dalam melindungi data pribadi (GDPR, art.45). Hingga saat ini, EC telah menyetujui sebelas yurisdiksi yang memiliki rezim perlindungan data yang dianggap sesuai standar atau memadai, yaitu Andorra, Argentina, Kanada, Kep. Faroe, Guernsey, Pulau Man, Israel, Jersey, Selandia Baru, Swiss, dan Uruguay.

2. Jika data tersebut berpindah ke luar wilayah Uni Eropa, yang tidak memiliki status 'kecukupan' dari EC, maka tingkat perlindungan data yang dijaga oleh organisasi/perusahaan penerima diharapkan setara dengan tingkat perlindungan yang berlaku di Uni Eropa, sesuai dengan persyaratan kontrak yang disepakati (GDPR, art. 46-47)

Hal ini bertujuan untuk melindungi privasi individu Uni Eropa terlepas dari mana pengendali data beroperasi. GDPR tidak hanya berlaku untuk organisasi/perusahaan besar atau yang berpendapatan tinggi, organisasi atau

perusahaan kecil yang mengolah data pribadi tetap harus mematuhi GDPR (Hoofnagle, Van Der Sloot, & Borgesius, 2023). Oleh karena itu, terlepas dari ukuran atau jenis organisasi yang terlibat, GDPR menekankan prinsip-prinsip perlindungan data yang lebih luas dan inklusif, serta fokus pada hak dan privasi individu. GDPR memiliki ketentuan yang sangat luas dalam hal ekstrateritorialitas, sebab peraturan tersebut berlaku bagi organisasi/perusahaan yang berbasis di luar Uni Eropa, tetapi masih berinteraksi dengan masyarakatnya (GDPR, art. 3 (1)). Aktivitas ini mencakup bisnis digital yang menyediakan layanan atau produk kepada individu di Uni Eropa (GDPR, art. 3 (2a)). GDPR juga menekankan bahwa penggunaan bahasa, mata uang lokal, penargetan konten atau iklan kepada masyarakat Uni Eropa dapat menunjukkan niat untuk menawarkan layanan kepada warganya (GDPR, rec. 23). Salah satu kasus yang relevan adalah Google Spain. Dalam kasus tersebut, walaupun nama perusahaan tersebut beroperasi di Spanyol, namun secara substansial dikendalikan oleh perusahaan induknya, Google INC. Oleh karena itu, CJEU memutuskan bahwa Google Spain masih dianggap sebagai bagian dari Google Inc yang berasal dari Amerika Serikat, yang artinya perusahaan tersebut tetap dianggap sebagai perusahaan asing dan diwajibkan untuk mematuhi hukum GDPR.

GDPR membuat perubahan besar pada cara platform teknologi mengumpulkan, menyimpan, dan mengelola data pribadi. Perubahan besar tersebut mencakup kebijakan dan praktik pengelolaan data yang ketat untuk memastikan kepatuhan terhadap GDPR. Hal ini dilihat dari GDPR berlaku untuk pihak ketiga yang melacak perilaku individu di Uni Eropa secara daring, seperti menempatkan *cookie* pelacakan di situs web atau aplikasi (GDPR, art.3 (2)). GDPR mengklasifikasikan praktik tersebut sebagai risiko tinggi, oleh karena itu, GDPR memberlakukan beban yang lebih

berat pada pihak ketiga yang terlibat dalam praktik tersebut (GDPR, rec. 24). Di sisi lain, GDPR memberikan perlakuan yang lebih ringan terhadap penggunaan data pihak pertama. Data pihak pertama adalah data yang dikumpulkan oleh pemilik situs web atau aplikasi yang dikunjungi oleh individu. GDPR mengakui banyak penggunaan data pihak pertama sebagai "sah" atau mematuhi peraturan dengan lebih mudah dibandingkan dengan penggunaan data oleh pihak ketiga (GDPR, art. 6 (1)). Dengan adanya ketentuan tersebut, organisasi/perusahaan diharapkan dapat melakukan evaluasi internal dengan teliti terhadap platform teknologi dan struktur datanya. Hal ini melibatkan pemahaman mendalam terhadap berbagai sistem informasi, situs web, basis data, gudang data, dan platform pengolahan data yang dimiliki.

Organisasi/perusahaan perlu memastikan bahwa keamanan yang memadai telah diimplementasikan secara bawaan (*by default*) dan sudah menjadi bagian integral dari desain sistem (*by design*). Selain itu, semua aktivitas yang melibatkan pemrosesan data pribadi harus dicatat secara rinci untuk memenuhi persyaratan GDPR. Dengan melakukan evaluasi internal, kemungkinan besar organisasi/perusahaan akan melakukan perubahan pada platform teknologi yang mencakup penyesuaian kebijakan keamanan, mengubah praktik periklanan, mengubah cara data disimpan dan dikelola, serta implementasi keamanan data yang lebih ketat sesuai dengan persyaratan GDPR. GDPR juga mewajibkan organisasi/perusahaan untuk menyediakan hak privasi yang kuat bagi penduduk Uni Eropa, seperti Hak untuk Dilupakan, Hak Akses Data, Hak Portabilitas Data, dan Hak Penjelasan tentang Pengambilan Keputusan Otomatis (Hoofnagle, Van Der Sloot, & Borgesius, 2023). Sebagai contoh, sebuah perusahaan besar seperti Alibaba mungkin menghadapi ribuan permintaan dari konsumen mengenai penggunaan data

pribadi. Pengguna dapat meminta akses ke data pribadi yang disimpan oleh platform tersebut. Dalam hal ini, Alibaba harus menyediakan prosedur yang memudahkan pengguna untuk mengajukan permintaan tersebut dan memberikan informasi yang jelas tentang data pribadi yang dikumpulkan (Hak Akses Data). Jika konsumen merasa tidak puas atau memiliki kekhawatiran terhadap cara Alibaba menangani data pribadinya, maka konsumen berhak untuk meminta penghapusan data tersebut (Hak untuk Dilupakan). Alibaba diwajibkan untuk meninjau dan merespons permintaan tersebut sesuai dengan persyaratan yang ditetapkan oleh GDPR. Selain itu, Alibaba juga harus menyediakan cara mudah bagi pelanggan untuk mentransfer data pribadi ke layanan lain, dengan menyediakan format data yang dapat diunduh atau disalin secara otomatis (Hak Portabilitas Data). Namun, saat menggunakan sistem tersebut, Alibaba harus memberikan penjelasan yang transparan kepada pengguna tentang dampak yang ditimbulkan (Hak Penjelasan tentang Pengambilan Keputusan Otomatis).

Dengan menerapkan langkah-langkah ini, dapat memastikan bahwa Alibaba mematuhi GDPR dan menjaga kepercayaan pelanggan. Penting bagi organisasi/perusahaan untuk menyempurnakan platform dan sistem teknologi yang sudah ada untuk memenuhi permintaan akses dan penghapusan data pribadi dari pelanggan. Perubahan pada platform teknologi, membuat perusahaan/organisasi menginvestasikan banyak tenaga kerja dan sumber daya untuk menyesuaikan GDPR. Biaya implementasi GDPR untuk organisasi/perusahaan cukup besar, sehingga hal ini dapat mengurangi keunggulan kompetitif perusahaan. Pasalnya, biaya implementasi GDPR kemungkinan akan diteruskan kepada konsumen melalui peningkatan harga produk atau layanan. Hal ini dapat mengurangi daya beli konsumen dan mempengaruhi daya saing perusahaan di

pasar yang kompetitif. Dengan demikian, implementasi GDPR tidak hanya berdampak pada keuangan perusahaan, tetapi juga dapat menghambat negara/perusahaan asing yang memiliki perlindungan data lemah, dan ingin berinvestasi di pasar Uni Eropa.

Mengingat Tiongkok merupakan kekuatan ekonomi global terkemuka, banyak perusahaan dari negara tersebut telah berbisnis dengan Uni Eropa. Perusahaan-perusahaan Tiongkok telah mencoba untuk mematuhi GDPR. Salah satu contohnya, Huawei, perusahaan telekomunikasi terbesar di Tiongkok yang memperluas pasar di Uni Eropa telah menunjuk petugas perlindungan data sebagai kepatuhannya terhadap GDPR. Namun, ada juga perusahaan Tiongkok yang tidak lagi beroperasi di Uni Eropa, yaitu Yeelight, perusahaan lampu canggih terbesar di Tiongkok. Berdasarkan forum Yeelight, perusahaan tersebut tidak lagi memberikan layanan kepada konsumen Uni Eropa, dengan alasan fitur yang disediakan tidak sesuai dengan penerapan GDPR (Ding, 2018). Kasus tersebut menandakan, penting bagi organisasi/perusahaan yang memperluas bisnis di pasar Uni Eropa untuk mematuhi dan mengikuti arahan GDPR. Sebab, hal ini dapat membantu organisasi/perusahaan untuk menghindari potensi denda dan risiko hukum yang timbul akibat pelanggaran terhadap GDPR.

4.3. Ekspansi Alibaba di Uni Eropa

Alibaba menjadi salah satu perusahaan *e-commerce* terbesar di dunia karena pendekatannya yang menghubungkan berbagai entitas dan memfasilitasi perdagangan lintas batas, serta lingkungan bisnis yang luas. Alibaba mencapai kesuksesannya melalui penerapan suatu model bisnis berbasis platform yang melibatkan kombinasi dari kemampuan digital dan aset fisik yang dimiliki oleh perusahaan tersebut. Kemampuan digital Alibaba meliputi, (1) *e-commerce* (Taobao, Tmall, Alibaba,

AliExpress, Juhuasuan, 1688, Lazada, Alitrip), (2) konten digital (Ali Cloud, Ali Music, Ali Sports, Tmall TV, Youku), (3) solusi digital (Alipay dan Alimama). Sementara aset fisik Alibaba meliputi, (1) jaringan distribusi (Cainiao Network), dan (2) toko fisik yang berfungsi sebagai *showroom* untuk produk/layanan yang ditawarkan di platform digital Alibaba. Dengan menggabungkan seluruh elemen tersebut, Alibaba telah menciptakan suatu lingkungan bisnis yang luas, di mana setiap bagian saling mendukung untuk menciptakan nilai tambah bagi seluruh sistem. Pendekatan seperti ini juga yang membantu Alibaba memperkuat posisinya sebagai pemimpin dalam industri *e-commerce* global (Wu & Gereffi, 2018).

Pada tanggal 26 April 2010, Alibaba meluncurkan AliExpress sebagai anak perusahaan yang pertama kali berlayar di pasar internasional. Peluncuran ini menjadi langkah awal Alibaba memasuki pasar Uni Eropa. AliExpress memungkinkan penjual kecil dan menengah dari Tiongkok dan negara-negara lain untuk menjual produknya kepada konsumen Uni Eropa. Untuk mencapai tujuan tersebut, platform ini menyediakan layanan dalam berbagai bahasa, seperti bahasa dari negara Rusia, Portugis, Spanyol, Perancis, Jerman, Italia, Belanda, dan Polandia, untuk memudahkan konsumen negara tersebut berbelanja secara daring (AliExpress, 2010)

Kemudian, Alibaba memulai kembali ekspansi pasarnya di Inggris dengan membuka kantor untuk membantu perusahaan-perusahaan lokal menjangkau konsumen Tiongkok melalui situs web, yaitu Tmall.com (Clark, 2016). Alibaba membuka kesempatan bagi pelaku usaha di Inggris untuk terlibat dalam kerja sama atau memanfaatkan platform dan layanan yang dimiliki oleh Alibaba. Tmall kemudian berkembang ke seluruh Eropa (Tmall Europe) yang fokusnya melayani merek lokal dan konsumen lokal di pasar local (EDCB, 2023). Pada bulan Juni 2023,

Tmall Europe dilaporkan sedang menjalankan proyek uji coba di Spanyol, dengan rencana untuk memperluas aplikasinya ke seluruh benua. Peluncuran Tmall di Eropa menunjukkan dedikasi Alibaba untuk membangun posisi kuat di wilayah tersebut (Livebuy, 2023).

Alibaba juga terlibat dalam kegiatan investasi aktif di berbagai sektor teknologi dan inovasi. Beberapa bidang investasinya meliputi teknologi keuangan, *cloud computing*, hiburan, olahraga, dan perawatan kesehatan. Pada tahun 2016, Alibaba mengekspansi bisnis *cloud computing* nya di salah satu negara anggota Uni Eropa, yakni Jerman. Alibaba Cloud menawarkan berbagai layanan *cloud computing* untuk penyimpanan data, analisis data, dan memberi solusi kecerdasan buatan (Alibabacloud, n.d.)

Hadirnya bisnis ini memberikan dampak positif pada infrastruktur teknologi informasi di wilayah Uni Eropa. Dengan membuka pusat data dan menyediakan layanan *cloud*, Alibaba memungkinkan perusahaan-perusahaan di Jerman untuk mengakses teknologi inovatif, memajukan transformasi digital, menerapkan teknologi canggih, dan meningkatkan efisiensi operasional (Xiao, 2016). Dilanjutkan pada tahun 2018, Alibaba Group Holding Ltd telah mengumumkan penandatanganan perjanjian dengan pemerintah Belgia untuk meluncurkan pusat perdagangan *e-commerce* (Farras, 2023). Pusat perdagangan ini mencakup investasi besar dalam infrastruktur logistik, Cainiao Network, yang mendukung operasional Alibaba di Belgia dan melayani kebutuhan konsumen di wilayah tersebut. Cainiao menyewa pelabuhan logistik seluas 220.000 meter persegi di bandara Liege, Belgia sebagai bagian dari kesepakatan strategi ini. Hal ini juga didukung oleh Alibaba yang menginvestasikan 100 juta Euro dalam proyek ini (Liu & Dubois, 2023) Melalui langkah tersebut, Alibaba berkomitmen untuk menciptakan peluang pertumbuhan ekonomi lokal, dan

mempercepat distribusi produk kepada konsumen di Uni Eropa.

Investasi dalam infrastruktur logistik juga mencerminkan strategi Alibaba untuk memperkuat rantai pasok globalnya, memastikan efisiensi dalam pengiriman, dan memberikan pengalaman berbelanja yang lebih baik bagi konsumen. Alibaba juga memperluas kehadirannya di Spanyol dengan peluncuran perusahaan Miravia pada tahun 2022 (Cordon, 2022). Miravia Spain menandai upaya Alibaba untuk menghadirkan platform digital serbaguna di Spanyol. Alibaba berambisi menciptakan ekosistem yang menggabungkan berbagai kategori produk, memungkinkan interaksi yang sinergis antara merek, konsumen, dan pembuat konten dalam satu tempat secara daring (EuropaPress, 2022) Melalui perusahaan ini, Alibaba berharap dapat memberikan konsumen pengalaman yang lebih kaya dan terhubung secara digital di pasar Spanyol.

4.4. Strategi Alibab dalam Menerapkan GDPR

AliExpress memasuki pasar Uni Eropa sebelum diberlakukan GDPR pada tahun 2018. Secara pada tahun tersebut belum ada pernyataan terkait AliExpress mematuhi regulasi yang berlaku. Namun, secara logika, saat itu AliExpress berhasil beroperasi di Uni Eropa selama bertahun-tahun, hal ini mengindikasikan bahwa AliExpress mematuhi undang-undang dan regulasi perlindungan data yang berlaku pada saat itu, yakni *Directive 95/46/EC*. Melalui aplikasinya, AliExpress memberikan informasi dan transparansi kebijakan privasi kepada pengguna terhadap pengelolaan data konsumen. AliExpress juga memberikan pengguna pilihan dan kontrol atas data pribadinya, termasuk opsi untuk menarik kembali persetujuan. Berdasarkan penelitian penulis, setelah 10 tahun berkembang, AliExpress mulai menyesuaikan kebijakan privasi dengan merancang ulang kebijakan-kebijakan, yang membahas cara data

konsumen ditangani dan dilindungi di era digital teknologi yang baru. Kebijakan ini dapat ditemukan di situs web atau aplikasi AliExpress bagian *Help Center*.

Melalui kebijakan tersebut, AliExpress memastikan keamanan dan privasi data pengguna di seluruh dunia merupakan prioritas utama bagi perusahaan. Kebijakan perlindungan data yang diterapkan AliExpress sesuai dengan standar internasional, termasuk GDPR. Seluruh data pengguna yang dikumpulkan tidak disimpan tanpa izin dan digunakan secara eksklusif untuk meningkatkan pengalaman berbelanja. AliExpress juga memberikan dokumen panduan untuk menjelaskan ketentuan yang lebih spesifik terkait: (1) pengumpulan informasi, (2) penggunaan data pribadi, (3) pengungkapan atau pembagian data pribadi, (4) retensi, (5) hak terkait data pribadi, (6) *cookies*, (7) ketentuan untuk anak di bawah umur, (8) tindakan keamanan, (9) perubahan kebijakan privasi, (10) pengunjung/konsumen dari Eropa dan Inggris, (11) pengunjung/konsumen dari AS, (12) pengunjung/konsumen dari Brasil, (13) transfer data pribadi internasional, (14) bahasa, dan (15) kontak yang dapat dihubungi (Aliexpress, 2022)

Selain itu, AliExpress juga menyediakan beberapa fitur untuk melindungi dan memberikan keamanan kepada konsumen saat melakukan transaksi. Beberapa diantaranya meliputi, (1) *Buyer Protection* untuk meningkatkan kepercayaan belanja dan melindungi pembelian konsumen, (2) *Escrow*, digunakan untuk meningkatkan keamanan transaksi, (3) *Dropshipping Agent*, mengurangi risiko stok dan biaya penyimpanan (Webster, 2020). AliExpress juga menyediakan beberapa pilihan metode pembayaran yang mempermudah konsumen Uni Eropa bertransaksi, seperti Carte Bleue (Perancis), QIWI (Rusia), WebMoney (Rusia), Yandex Money (Rusia), dan SMS (Rusia).

Sama seperti AliExpress, Miravia sebagai *e-commerce* yang baru hadir di Spanyol pada tahun 2022, cenderung mengikuti jejak AliExpress dalam menerapkan kebijakan yang sesuai dengan standar GDPR. Langkah tersebut diambil sejalan dengan prinsip-prinsip yang diatur GDPR untuk menjamin keamanan data pribadi konsumen Spanyol. Berlawanan dengan pendekatan AliExpress dan Miravia dalam menghadapi tantangan, strategi Tmall tidak terlalu mempengaruhi operasionalnya. Sebab, Tmall lebih berorientasi pada membantu perusahaan Uni Eropa mengakses preferensi konsumen di Tiongkok. Meskipun demikian, Tmall aktif berkolaborasi dengan pemangku kepentingan lokal, termasuk mitra bisnis, regulator, dan calon pelanggan.

Sedangkan strategi yang disusun oleh Alibaba Cloud adalah memanfaatkan keberhasilan dan pengalaman yang diperoleh di pasar Tiongkok sebagai modal utama. Maka dari itu, dukungan besar dari pemerintah Tiongkok dapat menjadi kunci sukses bagi Alibaba Cloud dalam mengembangkan bisnisnya. Pasalnya, pemerintah Tiongkok memiliki keinginan untuk terus mendukung pengembangan teknologi komputasi awan melalui dua program besarnya, yaitu “Made in China 2025” dan “Internet Plus”. Dengan pangsa pasar sekitar 40%, Alibaba Cloud berhasil memanfaatkan momentum digitalisasi yang mendominasi berbagai sektor di Tiongkok. Pangsa pasar yang kuat memberikan Alibaba Cloud keuntungan kompetitif sebagai pemimpin utama dalam menyediakan layanan *cloud computing* di Tiongkok. Oleh karena itu, Alibaba Cloud dianggap memiliki fondasi yang kuat untuk pertumbuhan dan perkembangan di masa depan. Posisi tersebut juga diperkuat oleh undang-undang keamanan siber baru di Tiongkok, yang mewajibkan perusahaan asing di Tiongkok menyimpan data di dalam negeri (KPMG, 2017) Perusahaan asing yang memilih untuk mematuhi regulasi ini dapat mengandalkan

infrastruktur teknologi canggih yang dimiliki oleh Alibaba Cloud untuk menyimpan dan mengelola datanya secara efisien di wilayah Tiongkok. Kebijakan ini menciptakan peluang bagi Alibaba Cloud untuk menjadi pilihan utama bagi perusahaan asing yang beroperasi di Tiongkok (KPMG, 2017).

Berdasarkan survei, tingkat keamanan data Alibaba Cloud dianggap rendah. Meskipun demikian, dampak dari evaluasi tersebut tidak berdampak besar bagi perusahaan tersebut. Sebab adanya pusat data lokal dianggap sebagai aspek positif yang memberikan dukungan strategis bagi Alibaba Cloud, sehingga perusahaan tetap mampu untuk mencapai kesuksesan di pasar *cloud computing*. "Pusat data lokal" merujuk pada penyimpanan data yang berada di suatu wilayah atau negara tertentu. Dengan ini, Alibaba Cloud dapat memberikan jaminan keamanan dan privasi data yang lebih tinggi kepada pelanggan. Alibaba Cloud mengatasi hal ini dengan memperluas keberadaannya secara internasional dan meluncurkan empat pusat data baru di Eropa, Australia, Timur Tengah, dan Jepang (Schnapp, 2017).

Untuk berhasil menembus pasar Jerman, Alibaba Cloud juga menyesuaikan strateginya dengan dinamika bisnis lokal yang unik. Salah satu pendekatan utama yang diambil oleh Alibaba Cloud adalah berkolaborasi dengan pemangku kepentingan setempat, baik itu mitra bisnis, regulator, atau pelanggan potensial. Alibaba telah bermitra dengan Accenture, IBM, Megaport, dan Eficode. Di Jerman, Alibaba Cloud bermitra dengan Vodafone untuk menempatkan pusat daya pertamanya di Frankfurt, dan pelanggan dapat membeli produk Alibaba Cloud melalui layanan Vodafone (Schnapp, 2017). Dengan membangun kemitraan yang kuat di tingkat lokal, Alibaba Cloud berusaha untuk memahami kebutuhan bisnis di Jerman dan menghadirkan solusi *cloud computing* yang relevan. Di samping itu, perusahaan ini juga

fokus pada inovasi produk dan layanan, memastikan bahwa penawaran perusahaan tidak hanya memenuhi standar internasional, tetapi juga dapat memenuhi ekspektasi tinggi dari pelanggan Jerman yang cenderung memiliki kebutuhan teknologi yang canggih. Selain itu, Alibaba Cloud aktif terlibat dalam inisiatif industri dan komunitas teknologi di Jerman. Faktanya, Alibaba Cloud juga mensponsori Olympic Games hingga tahun 2028 dalam sebuah kesepakatan yang bernilai 800 juta dollar AS. Sponsor ini menempatkan Alibaba di kelas yang sama dengan Coca Cola dan Samsung. dengan menyediakan layanan *cloud computing* dan analisis data untuk olimpiade (Shen, 2023) Strategi ini dapat memperkuat citra merek Alibaba Cloud sebagai platform yang dapat diandalkan dalam mendukung transformasi digital di negara tersebut.

Sebelum mempersiapkan diri untuk mematuhi GDPR, Alibaba Cloud berhasil memperoleh sertifikasi *TRUSTe Enterprise Privacy* dan memenuhi persyaratan *Personal Data Protection Act (PDPA)* Singapura. Pengalaman ini dianggap sebagai landasan persiapan Alibaba Cloud untuk mematuhi GDPR. Untuk memastikan kepatuhan dengan GDPR di Uni Eropa, terutama dengan persyaratan hak subjek data, Alibaba Cloud dengan cermat mengevaluasi setiap sistem dan aliran data untuk memastikan bahwa tidak ada bagian dari operasinya yang tidak mencakup persyaratan GDPR. Alibaba Cloud telah memodifikasi lebih dari seratus sistem yang digunakan. Alibaba Cloud juga telah berinvestasi besar-besaran dalam sumber daya manusia dan sumber daya teknis, baik itu konsultan eksternal maupun tim proyek internal, dan berkoordinasi di antara berbagai departemen. Pada saat yang sama, Alibaba Cloud juga menggunakan platform privasi untuk secara sistematis mengelola dan menjaga operasi privasi. Melalui situs web resmi, Alibaba Cloud juga menjelaskan secara rinci bagaimana

sistemnya menerapkan peraturan GDPR: (Alibabacloud, n.d.)

1. Alibaba Cloud mematuhi GDPR Pasal 12. Alibaba Cloud berkomitmen untuk melindungi informasi pribadi pelanggan dan menjamin bahwa informasi tersebut hanya digunakan untuk tujuan yang disetujui oleh pelanggan. Kebijakan privasi Alibaba Cloud sepenuhnya transparan untuk publik dan dapat ditemukan di situs resminya.

2. Alibaba Cloud mematuhi GDPR Pasal 17 tentang Hak untuk Dihapus. Alibaba Cloud menyediakan fungsi penghapusan akun, yang mencapai penghapusan akun secara sistematis.

3. Alibaba Cloud mematuhi GDPR Pasal 25 tentang Privasi dengan Desain. Semua produk terbaru Alibaba Cloud telah melalui tinjauan keamanan dan penilaian desain privasi untuk memastikan pertimbangan keamanan dan privasi tertanam dalam produk.

4. Alibaba Cloud mematuhi GDPR Pasal 32 tentang Keamanan. Alibaba Cloud telah mempublikasikan versi terbaru dari metodologi keamanan *whitepaper*, yang mencakup kebijakan keamanan, keamanan organisasi, kepatuhan, keamanan data, kontrol akses, keamanan personel, keamanan fisik, keamanan infrastruktur, pengembangan dan pemeliharaan sistem dan perangkat lunak, pemulihan bencana, dan kontinuitas bisnis.

Pada Desember 2018, Alibaba Cloud menjadi penyedia *cloud* pertama yang menunjukkan kesesuaian dengan persyaratan tambahan dari standar keamanan Jerman C5. Hal ini bertujuan untuk menunjukkan komitmen perusahaan terhadap standar keamanan yang lebih tinggi. Selain itu, Alibaba Cloud telah menetapkan kebijakan dan prosedur pemberitahuan pelanggaran, dan telah melakukan berbagai latihan untuk memastikan tim terlibat sadar akan peran dan tanggung jawab masing-masing.

Alibaba Cloud juga merupakan anggota pendiri dari EU Cloud Code of

Conduct dan General Assembly, yang secara aktif terlibat dalam pembentukan kode etik untuk layanan *cloud* di Uni Eropa sesuai dengan persyaratan Pasal 40 GDPR. Alibaba Cloud berkolaborasi dengan Departemen Perlindungan Data, untuk memastikan panduan GDPR diterapkan saat merancang kode. Alibaba Cloud berkomitmen untuk menjaga standar tinggi perlindungan data di seluruh ekosistem dan berkontribusi pada perkembangan industri teknologi yang sehat. Alibaba Cloud juga mendukung transparansi dalam industri *cloud computing*, dan membantu pelanggan *cloud* memahami cara penyedia layanan *cloud* menangani masalah perlindungan data. Sebab transfer lintas batas data pribadi menjadi tantangan yang dihadapi banyak perusahaan global, terutama dalam era pertumbuhan cepat layanan *cloud*. Tidak semua alat transfer yang disetujui Uni Eropa sesuai dengan model bisnis yang terus berubah.

Oleh karena itu, *European Commission* memutuskan untuk memulai kembali Kontrak Model Standar untuk pemroses data dan sub-pemroses. Kontrak Model Standar ini merupakan kerangka kerja hukum yang digunakan untuk melindungi data pribadi yang ditransfer di antarnegara atau wilayah yang berbeda. Terdapat sebuah kelompok yang bertugas memberikan saran dan panduan kepada EC terkait dengan perlindungan data dan privasi yang tertuang pada Kelompok Kerja Pasal 29. Alibaba Cloud bersama dengan beberapa rekan lainnya, memutuskan untuk bergabung dalam kelompok yang dibentuk untuk membantu menciptakan alat transfer data baru. Alat ini dirancang untuk membantu industri mengatasi tantangan transfer lintas batas data pribadi yang lebih sesuai dengan perkembangan model bisnis yang terus berubah. Dengan bergabung dalam kelompok tugas ini, Alibaba Cloud berpartisipasi aktif dalam membentuk solusi untuk masalah ini dan mendukung perkembangan regulasi yang relevan (Alibabacloud, n.d.)

5. Kesimpulan

Uni Eropa merupakan negara yang memiliki regulasi perlindungan data yang dituangkan dalam General Data Protection Regulation (GDPR). Sebagai studi kasus, Alibaba memenuhi seluruh kriteria pelanggaran yang ditegakkan oleh GDPR. Secara keseluruhan, hubungan Uni Eropa dan Alibaba dibangun atas dasar perkembangan hubungan ekonomi yang kuat antara Uni Eropa dan Tiongkok. Mereka berkembang menjadi aktor penting dalam perdagangan internasional, dengan menciptakan sifat interdependensi dan menekankan kepentingan bersama. Perlindungan privasi konsumen di Uni Eropa bermula dari fokus utama institusi internasional dan kemudian diwujudkan dalam bentuk Directive 95/46/EC. Namun, penerapan Direktif di negara anggota tidak merata dan tidak dapat menyesuaikan kemajuan teknologi, maka dibentuklah General Data Protection Regulation (GDPR) yang memiliki cakupan luas dan komprehensif. GDPR memberi persyaratan tinggi untuk organisasi atau perusahaan lokal maupun asing yang mengolah data pribadi di Uni Eropa. Negara atau perusahaan yang memiliki masalah privasi atau tidak memiliki perlindungan data yang memadai, dilarang untuk mengakses data pribadi penduduk setempat.

Apabila entitas tidak mematuhi regulasi tersebut, maka akan dijatuhkan sanksi finansial yang bersifat administratif dan regulatif. Sanksi yang berlaku akan ditegakkan oleh Data Protection Authorities (DPAs) dari masing-masing negara anggota. Untuk mencapai kesuksesan global, Alibaba memperluas bisnisnya dengan menanam anak-anak perusahaannya di pasar Uni Eropa. Dalam memperluas operasionalnya,

Alibaba dihadapi tantangan yang melibatkan aspek pembentukan regulasi terkait perlindungan privasi dan keamanan data pribadi konsumen, penyesuaian sistem pembayaran dan preferensi konsumen, persaingan lokal, infrastruktur logistik,

serta penerimaan konsumen. Dalam mengatasi tantangan tersebut, AliExpress, Miravia, dan Cainiao membentuk kebijakan privasi data konsumen yang sesuai dengan standar GDPR dan mencantumkannya di websiteresmi. Sedangkan Tmall yang memiliki fokus berbeda, berorientasi pada kolaborasi pemangku kepentingan lokal. Berbeda dari anak perusahaan lain, Alibaba Cloud menghadapi tantangan yang lebih berat. Hal ini disebabkan orientasi utama perusahaan pada penyimpanan dan pengolahan data.

Dalam menghadapi tantangan tersebut, Alibaba Cloud memanfaatkan keberhasilan dan pengalaman yang diperoleh di Tiongkok sebagai modal utama. Untuk membangun tingkat keamanan data yang terpercaya, Alibaba Cloud memperluas keberadaannya dengan meluncurkan pusat penyimpanan data di berbagai negara.

Sebagai persiapan mengeluarkan regulasi yang sesuai standar GDPR, Alibaba Cloud berhasil memperoleh sertifikasi TRUSTe Enterprise Privacy dan memenuhi persyaratan Personal Data Protection Act (PDPA) Singapura sebagai fondasi kepercayaan. Alibaba Cloud juga berinvestasi besar-besaran dalam sumber daya manusia dan sumber daya teknis untuk mengevaluasi sistem dan aliran data.

Dari penelitian ini, akhirnya dapat menjawab rumusan masalah terkait penerapan GDPR terhadap perusahaan asing, dan strategi Alibaba yang memenuhi kriteria pelanggaran GDPR. Prosedur yang diterapkan GDPR tergolong ketat, namun dalam penerapannya masih terdapat celah yang menjadi peluang bagi perusahaan asing untuk beroperasi ke pasar Uni Eropa. Alibaba sebagai salah satu perusahaan yang berhasil mematuhi GDPR dan mengembangkan banyak anak perusahaannya di Uni Eropa. Usaha dan kegigihan Alibaba dalam memperbaiki masalah internalnya, meningkatkan nilai, dan citranya di negara asal. Alibaba mendapatkan dukungan penuh dari

pemerintah Tiongkok yang menjadikan Alibaba sebagai perusahaan yang sangat diandalkan. Alibaba membuktikan bahwa dengan fondasi yang kuat dapat membantunya mematuhi GDPR, bahkan mempengaruhi Tiongkok untuk menciptakan sebuah regulasi yang sekelas dengan GDPR.

DAFTAR PUSTAKA

- Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in E-Commerce: Examining User Scenarios and Privacy Preference. *ACM Conference on Electronic Commerce* (pp. 1-8). ACM.
- Alibabacloud. (n.d.). *GDPR*. Retrieved from Alibabacloud: <https://www.alibabacloud.com/id/trust-center/gdpr>.
- AliExpress. (2010). *AliDExpress Store*. Retrieved from Aliexpress: <https://www.aliexpress.com/store/1100302029>.
- Aliexpress. (2022). *AliExpress.com Privacy Policy*. Retrieved from Aliexpress.com: https://terms.alicdn.com/legal-agreement/terms/suit_bu1_alibaba/suit_bu1_alibaba201909171350_82407.html?spm=service_hall.24300481.0.0.2f144300Z0eKqd.
- Binding, J., & Purnhagen, K. (2011). Regulations on E-Commerce Consumer Protection Rules in China and Europe Compared- Same but Different? *JIPITEC* 3, 187-193.
- Bisson, D. (2023). *Misconfigured Elasticsearch Cluster Exposed over 90 Million Records*. Retrieved from Tripwire: www.tripwire.com/state-of-security/misconfigured-elasticsearch-cluster-exposed-over-90-million-records.
- Budnitz, M. E. (1998). Privacy Protection for Consumer Transaction in Electronic Commerce. *South Carolina Law Review*, vol. 49, 860-869.
- Clark, D. (2016, September 26). *How Jack Ma Built One of the World's Biggest Companies*. Retrieved from British Council: <https://www.britishcouncil.org/voices-magazine/how-jack-ma-built-one-worlds-biggest-companies>.
- Cordon, M. (2022, December 1). *Alibaba Launches Ecommerce Platform in Spain*. Retrieved from Tech in Asia: <https://www.techinasia.com/alibaba-subsiidiary-launches-ecommerce-platform-spain>.
- Ding, Y. (2018, May 18). *Announcement: European Server Service Will Be Restored within a Week*. Retrieved from Yeelight Forum: <https://forum.yeelight.com/t/announcement-european-server-service-will-be-restored-within-a-week/5344>.
- EDCB. (2023, October). *Alibaba Ecosystem: Alibaba Group, Tmall, Taobao & Their Success in eCommerce*. Retrieved from EDCB: <https://ecommercedb.com/insights/alibaba-insights-chinas-commerce-giant/3447>.

- EuropaPress. (2022, December 2). *Alibaba Launches Miravia in Spain, a New Fashion, Beauty and Lifestyle Marketplace*. Retrieved from Fashion Network: <https://www.techinasia.com/alibaba-subsiary-launches-ecommerce-platform-spain>.
- EUROSTAT. (2023). *Euro Area Consumer Spending*. Retrieved from Trading Economics: <tradingeconomics.com/euro-area/consumer-spending>.
- Farras, B. (2023, December 5). *Buka Hub di Belgia, Alibaba Ekspansi Pasar Eropa*. Retrieved from CNBC Indonesia: <https://www.cnbcindonesia.com/news/20181205204218-4-45151/buka-hub-di-belgia-alibaba-ekspansi-pasar-eropa>.
- Fienberg, S. E. (2006). Privacy and Confidentiality in an E-Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation. *Statistical Science* 21, no. 2, 1-3.
- GDPR, A. 4. (2018). *Art. 44 GDPR, " General Data Protection Regulation (GDPR)*. Retrieved from gdpr-info.edu: <gdpr-info.eu/art-44-gdpr/>.
- Goh, B. (2022, July 6). *Hackers Claims to Have Stolen 1 Bln Reords of Chinise Citizens from Police*. Retrieved from Reuters: <www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinise-citizens-police-2022-07-04/>.
- Gunther, O., Spiekermann, S., & Berendt, B. (2005). Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. *ResearchGate*, 1-7.
- Guo, M. (2021). A Comparative Study on Consumer Right to Privacy in E-Commerce. *Modern Economy* 03, no. 04, 402-407.
- Hess, B., & Mariottini, C. M. (2015). Foreword. In Hess, B. Hess, & C. M. Mariottini, *European and American Developments: Protecting Privacy in Private International and Procedural Law and by Data Protection*. Baden-Baden: Nomos.
- Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2023). The European Union General Data Protection Regulation: What It Is And... *Information & Communications Technology Law*.
- Ishmael, L. (2020). Soft Power & Global Ambition: The Case of China's Growing Reach in Europe. *Horizon Insights* 3, no. 2, 10-29.
- Kharpal, A. (2023, June 15). *Alibaba to Launch Local Versions of Its China E-Commerce Site in Europe*. Retrieved from CNBC: <www.cnbc.com/2023/06/15/alibaba-to-launch-local-version-of-china-e-commerce-site-tmall-in-europe.html>.

KPMG. (2017). *Overview of China's Cybersecurity Law*. KPMG China.

Lin, P. (2021). Electronic Commerce and Its Regulation In The European Union and China: A Comparative Analysis. *People's Friendship University of Russia*, 38-43.

Liu, O., & Dubois, L. (2023, October 5). *Alibaba Accused of "possible Espionage" at European Hub*. Retrieved from Financial Times:
<https://www.ft.com/content/256ee824-9710-49d2-a8bc-f173e3f74286>.

Livebuy. (2023, June 26). *Alibaba's Tmall on the Way to Europe*. Retrieved from Medium:
<https://medium.com/@livebuy.io/alibabas-tmall-on-the-way-to-europe-6b2da98d15ee>.

Millward, S. (2015, December 1). *Alibaba Opens Offices in France and Germany as It seeks New Goodies for Chinese Consumers*. Retrieved from Tech in Asia- Connecting Asia's Startup Ecosystem: www.techinasia.com/alibaba-cross-border-ecommerce-france-germany.

Muneer, A., & Farooq, Z. (2018). Data Privacy Issues and Possible Solutions in E-Commerce. *Journal of Accounting & Marketing* 07, no. 03, 1-3.

O'Neill, A. (2023, October 5). *European Union (EU)- Total Population 2022*. Retrieved from Statista: www.statista.com/statistic/253372/total-population-of-the-european-union-eu/.

Partridge, M. (2022, July 20). The Fallout from Alibaba's Huge Data Breach. *MoneyWeek*.

Rosadi, S. D., & Pratama, G. G. (2018). Perlindungan Privasi Dan Data Pribadi Dalam Era Ekonomi Digital Di Indonesia. *Journal Unpar* 4, no.1.

Schnapp, S. (2017). *Alibaba's Ambition to Become a Global Player in Cloud Computing*. Zurich University of Applied Sciences.

Schoukens, H., & Bastmeijer, K. (2014). Species Protection In The European Union: How Strict Is Strict? In C. H. Born, A. Cliquet, H. Schoukens, D. Misonne, & G. Van Hoorick, *The Habitats Directive in Its EU Environmental Law Context: European Nature's Best Hope?* Oxford: Routledge, Abingdon.

Shen, X. (2023). Exclusive: Alibaba Cloud's Founder Looking Forward to Supporting Paris Olympic 2021. *South China Morning Post*.

Simamora, C. M. (2017). *E-Commerce*. Pusdiklat Aparatur Perdagangan- Kementerian Perdagangan.

- Terzi, N. (2011). The Impact of E-Commerce on International Trade and Employment. *Procedia- Social and Behavioral Sciences*.
- Vecchi, A., & Brennan, L. (2022). Two Tales of Internationalization- Chinese Internet Firms' Expansion into the European Market. *Journal of Business Research* 152, 106-127.
- Voss, W. G., & Dumas, H. B. (2021). EU General Data Protection Regulation Sanction in Theory and in Practice. *Santa Clara Computer and High Technology Law Journal*, 14-44.
- Wang, R. (2018). *Internationalization Strategy of Chinese E-Commerce Firms: The Case of Alibaba Group*. Retrieved from dspace.spbu:
https://dspace.spbu.ru/bitstream/11701/12996/1/Mater_Thesis-Wang_Rui.pdf.
- Webster, S. (2020, June 26). *AliExpress' History and Its Expansion to Latin America: Labs*. Retrieved from LABS: <https://labsnews.com/en/articles/business/why-the-nine-year-rise-of-aliexpress-means-big-plans-for-latin-american-ecommerce/>.
- Wiranjaya, I. A., & Ariana, I. P. (2017). Perlindungan Hukum Terhadap Pelanggaran Privasi Konsumen Dalam Bertransaksi Online. *Kertha Semaya: Jurnal Ilmu Hukum* 6, no. 1.
- Wu, X., & Gereffi, G. (2018). International Business in the Information and Digital Age. *Emerald Insight*.
- Xiao, E. (2016, November 21). *Alibaba Cloud Races Ahead with Global Expansion, Adds 4 more Countries to Its Portfolio*. Retrieved from Tech in Asia:
<https://www.techinasia.com/alibaba-cloud-races-global-expansion-adds-3-countries-portfolio>.
- Yang, C. (2011). Analysis on Protection of E-Commerce Consumer Network Privacy. *Procedia Engineering*, 5519-5523.